City of Las Vegas

I.T. Governance

Last Updated: 04/28/2005

TABLE OF CONTENTS

SECTION 1 - INTRODUCTION 5

1.1 STATEMENT OF PURPOSE 6
1.2 DEFINITION 6
1.3 WHY HAVE AN I.T. GOVERNANCE PROGRAM? 6
1.4 I.T. GOVERNANCE MODEL 7

SECTION 2 - ORGANIZATION 9

2.1 INFORMATION TECHNOLOGIES (I.T.) ORGANIZATION 10
2.2 ADMINISTRATION 12
2.3 STAFF SERVICES 13
2.4 ENTERPRISE PROJECT MANAGEMENT 14
2.5 APPLICATIONS SERVICES 15
2.6 CLIENT RELATIONSHIP SERVICES 20
2.7 SYSTEMS INFRASTRUCTURE MANAGEMENT 24

SECTION 3 - KEY I.T. GOVERNANCE FUNCTIONS 26

3.1 APPLICATIONS MANAGEMENT 27
3.2 APPLICATIONS TESTING 35
3.3 ASSET MANAGEMENT 38
3.4 BUDGET AUTHORITY 42
3.5 BUDGET PLANNING AND PROCESS 44
3.6 BUSINESS ANALYSIS 49
3.7 CAPACITY PLANNING 51
3.8 CHANGE MANAGEMENT 53
3.9 COMMUNICATIONS MANAGEMENT 57
3.10 COMPUTER OPERATIONS 63
3.11 COST ALLOCATION 67
3.12 DATA MANAGEMENT 69
3.13 DESKTOP SUPPORT 74
3.14 eGOVERNMENT PLANNING AND ADMINISTRATION 78
3.15 NETWORK MANAGEMENT 82
3.16 PORTFOLIO MANAGEMENT 85
3.17 PROJECT MANAGEMENT 89
3.18 QUALITY ASSURANCE 96
3.19 REFERENCE 99
3.20 RESOURCE MANAGEMENT 101
3.21 SECURITY AND CONTINGENCY PLANNING 104
3.22 SERVICE LEVEL AGREEMENTS (SLAs) 108
3.23 STRATEGIC PLANNING 111

TABLE OF CONTENTS

3.24 SYSTEMS ADMINISTRATION 113
3.25 TECHNICAL ARCHITECTURE 117

SECTION 4 - I. T. GOVERNANCE-RELATED POLICIES, PROCEDURES, & GUIDELINES 121

4.1 AUDIO/VISUAL EQUIPMENT POLICY/PROCEDURE 122
4.2 COMMUNICATIONS EQUIPMENT POLICY 123
4.3 COMMUNICATIONS EQUIPMENT PROCEDURE 124
4.4 E-MAIL POLICY 127
4.5 E-MAIL RECORDS POLICY 129
4.6 INCIDENT MANAGEMENT PROCEDURE 133
4.7 INFORMATION RESOURCES USE POLICY 136
4.8 INTERNET POLICY 139
4.9 INTERNET PROCEDURE 141
4.10 INTERNET WEB SITE CONTENT MANAGEMENT POLICY 144
4.11 INTRANET POLICY 147
4.12 INTRANET PROCEDURE 149
4.13 INTRANET WEB SITE CONTENT MANAGEMENT POLICY 150
4.14 I.T. ACCESS PROCEDURE 153
4.15 I.T. CONFIGURATION CONTROL COMMITTEE CHANGE REQUEST PROCEDURE 155
4.16 MICROCOMPUTER HARDWARE POLICY 157
4.17 MICROCOMPUTER SOFTWARE POLICY 160
4.18 PURCHASED SOFTWARE EVALUATION GUIDELINES 164
4.19 REPORT REQUEST POLICY 168
4.20 REPORT REQUEST FORM PROCEDURE 169
4.21 REPORTING MICROCOMPUTER PROBLEMS 170
4.22 SOFTWARE CHANGE CONTROL POLICY 172
4.23 SOFTWARE DEVELOPMENT LIFE CYCLE POLICY 175
4.24 SOFTWARE TESTING POLICY 179
4.25 SOFTWARE TESTING PROCEDURE 182
4.26 SOURCE CODE MANAGEMENT POLICY 187
4.27 USER ACCOUNT TERMINATION PROCEDURE 189
4.28 VERSION CONTROL POLICY 191
4.29 WEB SITE PRIVACY POLICY 194

SECTION 5 - APPENDIX 197

5.1 I.T. CONFIGURATION CONTROL COMMITTEE CHARTER 198
5.2 ORACLE APPLICATIONS CONTROL PROCESS 208

TABLE OF CONTENTS

5.3 ITCCC REQUEST FORM 212
5.4 I.T. REQUEST FORM 213
5.5 SAMPLE BUDGET PREPARATION WORKSHEET 215
5.6 CLV STANDARD PROJECT PROCESS STEPS 218
5.7 SAMPLE INTERNET HOME PAGE 222
5.8 SAMPLE INTRANET HOME PAGE 223
5.9 SAMPLE CLIENT SUPPORT INTRANET HOME PAGE 224
5.10 SAMPLE INTERNET GIS APPLICATION WEB PAGES 225

SECTION 1 - INTRODUCTION

FEATURED IN THIS SECTION

1.1 STATEMENT OF PURPOSE

1.2 DEFINITION

1.3 WHY HAVE AN I.T. GOVERNANCE PROGRAM?

1.4 THE GOVERNANCE MODEL

INTRODUCTION

1.1 STATEMENT OF PURPOSE

Information Technologies (I.T.) is charged with achieving "solutions that meet or exceed the needs of the city and its citizens." Fulfilling this support mission can be strengthened by:

- Identification and documentation of key functionality criteria that govern how I.T. conducts business
- Establishment of appropriate policies, procedures, guidelines, and work rules, where necessary, to ensure that the business functions are carried out correctly, thoroughly, and efficiently.

The term 'governance' addresses the proper management of internal organizations with the objective of helping to achieve the stated goals of the enterprise. 'I.T. governance' takes these concepts one step further down in the hierarchy and applies them to the I.T. organization. The purpose of I.T. governance is to:

- Direct I.T. endeavors such that both I.T. and the enterprise are enabled to:
  - achieve stated goals
  - exploit opportunities (for example, to change project priorities or to reassign personnel)
  - maximize benefits
- Ensure that:
  - I.T. resources are used responsibly
  - I.T.-related risks are identified and managed appropriately

1.2 DEFINITION

I.T. Governance – The utilization of I.T. processes and enterprise relationships to better enable the enterprise to achieve its goals and objectives by providing the structure linking I.T. processes, resources, and information.

1.3 WHY HAVE AN I.T. GOVERNANCE PROGRAM?

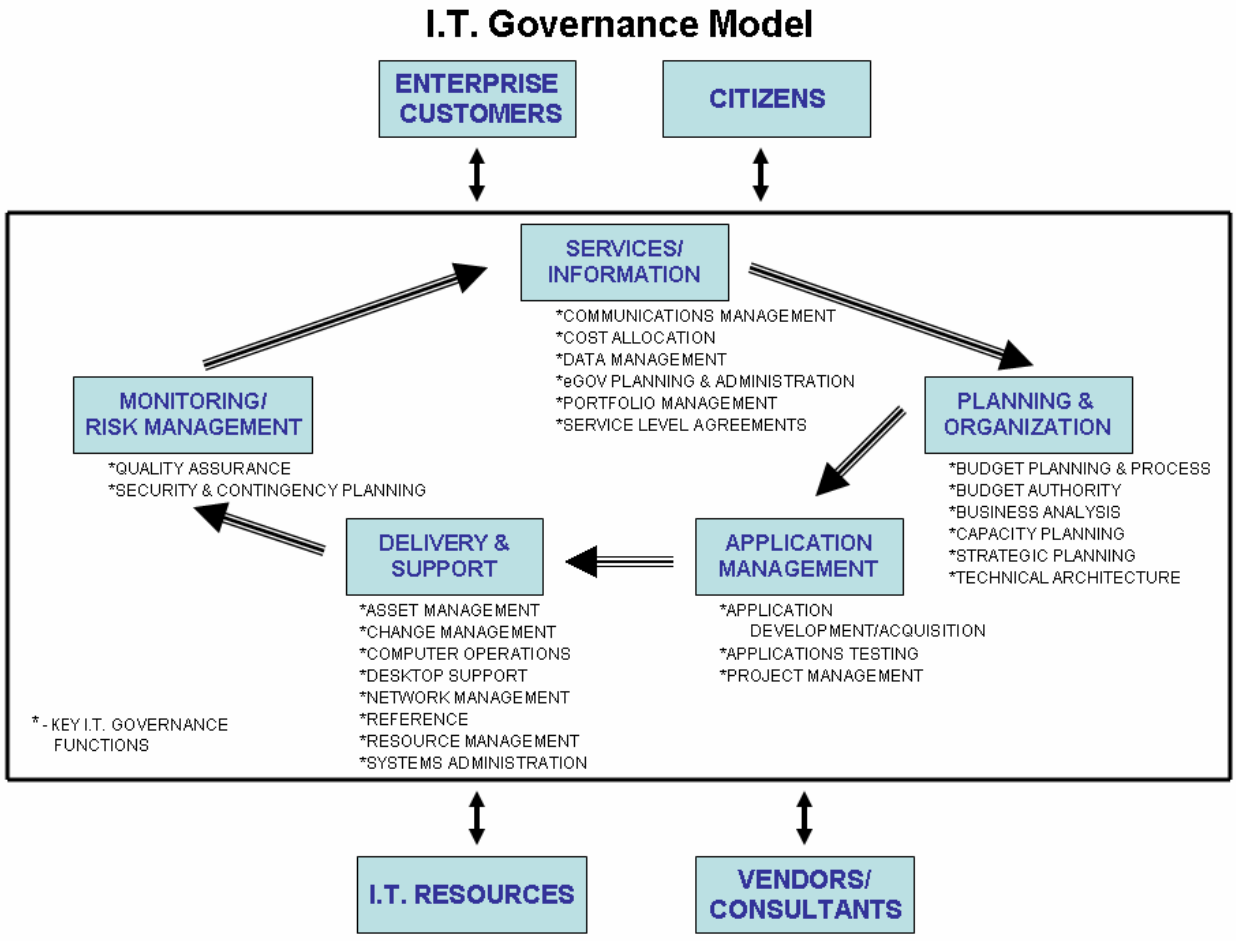
We already are using governance principles each time we acquire products or engage in outsourcing. Typically we do the diligence necessary to determine if the vendor's products have met other customers' expectations in the past, if products are delivered on time, if contractual obligations are met, etc. When outsourcing, we carefully define service levels, processes, and responsibilities. If we are seeking to satisfy ourselves that another entity's products and services can live up to our expectations, shouldn't we seek the same from an internal organization as critical to enterprise success as I.T? Over the years I.T. has been recognized as necessary and fundamental for resource management.

INTRODUCTION

Today I.T. is viewed as indispensable for customer relationship management. E-government portals now dispense information and services to customer groups as diverse as citizenry, internal departments, and employees. Ensuring that these customer interfaces are managed responsibly is an all-important function of I.T. Governance.

1.4 I.T. GOVERNANCE MODEL

The I.T. Governance Model below shows how principal management areas of I.T. are supported by key I.T. governance functions.



INTRODUCTION

Today I.T. Governance seeks to support the enterprise strategically by aligning its goals with those of the enterprise. This means I.T. must form a strategic partnership with management in which enterprise goals and objectives are always known and well-communicated to I.T. staff.

SECTION 2 - ORGANIZATION

FEATURED IN THIS SECTION

2.1 INFORMATION TECHNOLOGIES (I.T.) ORGANIZATION

2.2 ADMINISTRATION

2.3 STAFF SERVICES

2.4 ENTERPRISE PROJECT MANAGEMENT

2.5 APPLICATIONS SERVICES

2.6 CLIENT RELATIONSHIP SERVICES

2.7 SYSTEMS INFRASTRUCTURE MANAGEMENT

ORGANIZATION

2.1 INFORMATION TECHNOLOGIES (I.T.) ORGANIZATION

I.T. is organized into functional areas that support its mission, goals, and objectives. During the 'mainframe' era, the city's computer services were provided by Information Systems, a Division of Finance. At that time, most I.T. shops were classically divided into systems, programming, and operations groups and the same held true for the city of Las Vegas. This was a satisfactory arrangement when the primary job of I.T. was to produce 'batch' computer programs that read through batches of records each evening to produce reports for management as well as bills and receipts for external customers. One of our biggest user departments has always been Municipal Courts. Within this application, with one pass through the courts' files each night, one massive program generated more than 20 print files of traffic and criminal-related forms and receipts for mailing, as well as reports for management.

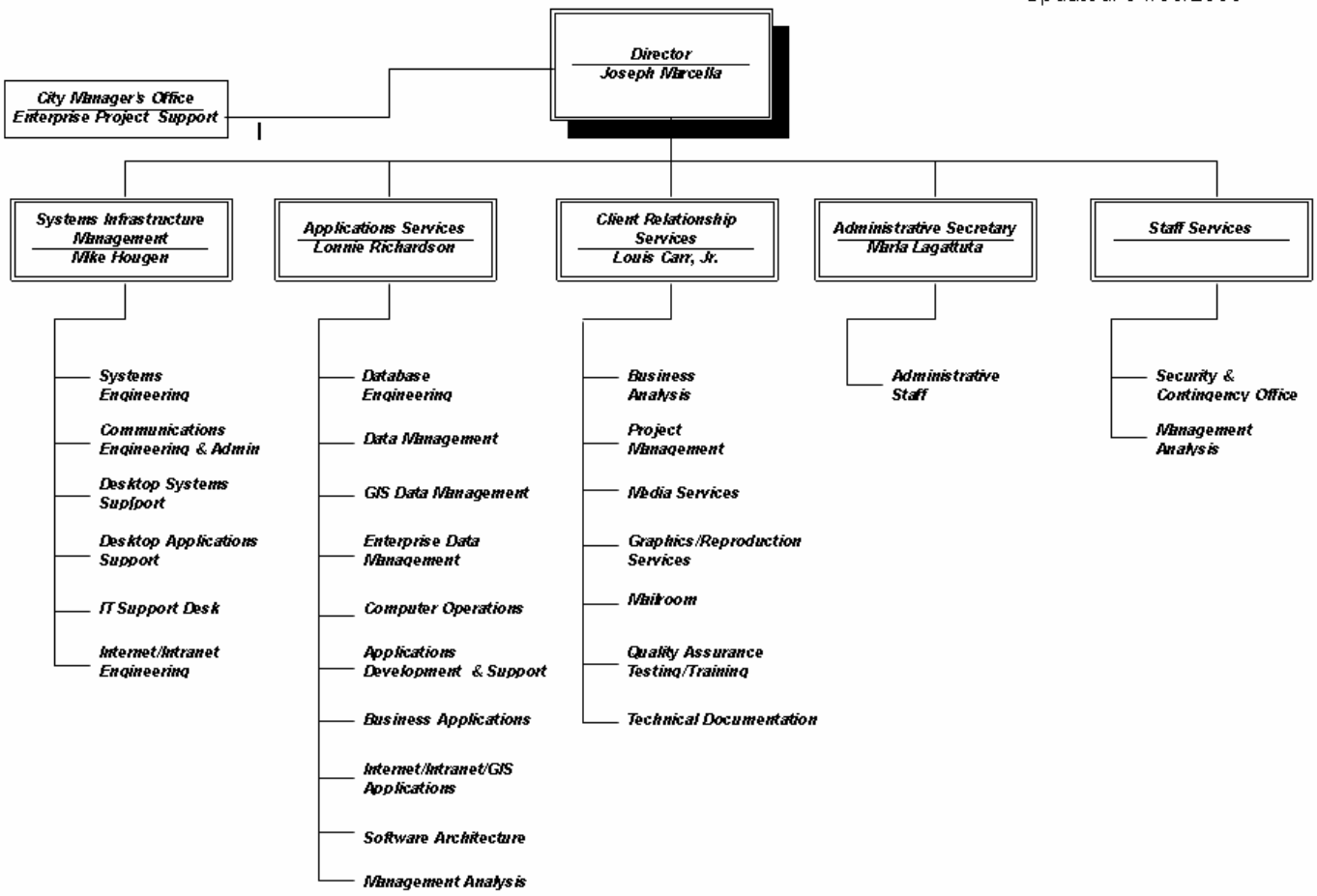
In 1997, the focus shifted from mainframe computers wired to a network of 'dumb' terminals to a 'client-server' arrangement in which powerful server computers containing the database files were linked to departmental 'client' personal computers containing programs for updating and extracting data from the centrally-stored information.

While client-server applications are still used internally, today's preferred method of disseminating and updating information is via online 'web' networks that provide services to anyone with a personal computer. The focus of I.T. has now become that of a 24 hour-per-day information and online-updating provider for not only city departments but citizens directly. New divisional groupings have been formulated to more efficiently manage and secure this wealth of information. The groups are: administration, staff services, client relationship services, applications, and systems infrastructure. An all-important liaison with the City Manager's Office helps to make enterprise projects run more smoothly rather than having I.T. exclusively attempt to coordinate these projects among multiple departments with separate and sometimes conflicting objectives.

ORGANIZATION

Information Technologies Department

Updated: 04/05/2005



ORGANIZATION

2.2 ADMINISTRATION

I.T. Administration is at the forefront of the organizational components by (1) providing guidance and direction to all staff in the form of the Director of Information Technologies and (2) helping all of the facets work together and run smoothly with dedicated and capable administrative staff. An Administrative Secretary assists the director, and office specialists work together to support the other divisional groups.

The director not only ensures that I.T. goals are aligned with those of the organization but works with other local government entities to pursue interaction for dealing with common problems. Then, on the national level, our director belongs to MIX (Metropolitan Information eXchange), an Internet-based group of I.T. directors from local governments, who are constantly trading job descriptions, organizational reports and advice on common I.T. issues.

The administrative staff helps to coordinate activities ranging from equipment setups for meetings to taking meeting minutes to arranging monthly birthday celebrations and annual I.T. picnics to contribute to morale and promote employee cooperation.

ORGANIZATION

2.3 STAFF SERVICES

Staff Services are vital organizational elements providing for security and contingency planning in addition to research, reporting, and recommendations to management.

2.3.1 SECURITY AND CONTINGENCY OFFICE

In the early years of data processing, security and protection of data in standalone mainframes was most concerned with hardware failures or improper backup procedures. As networking became more widespread, security was more concerned with stolen data. Now, web-networked files have to be protected from individuals who want to destroy data just for the 'fun of it.'

Also, active contingency planning has to be continually forged to prepare for potential disasters, from natural to man made. CLV information security and contingency planning is maintained by the Security and Contingency Office, staffed by the Information Security and Contingency Administrator. This key position reports directly to the department director.

2.3.2 MANAGEMENT ANALYSIS

These are the staff members that are depended upon when statistical spreadsheets and graphs for web posting, reports for senior management, etc. are needed. Guidance for web functionality, standards, and consistency also reside within this group's purview.

ORGANIZATION

2.4 ENTERPRISE PROJECT MANAGEMENT

Enterprise projects are those involving users across departmental lines. At the city, this includes Oracle Financial and Human Resources systems, and Hansen application systems serving Business Services, Public Works, Planning and Development and Building and Safety functions. These projects are managed by a lead Administrative Officer from the City Manager's Office and staffed with Enterprise Project Managers from within I.T. Both the Oracle and Hansen groups employ dedicated change control committees for approving modifications to the Test and Production environments. Samples of online change request documents for these groups are shown in the appendix. Committee members consist of lead users from each of the affected departments. Approval coordination and logging is performed by I.T.'s quality assurance staff.

ORGANIZATION

2.5 APPLICATIONS SERVICES

Applications Services is divided into four functional areas, one that directly interfaces with users and three that operate in the background in support roles:

- Database Engineering
- Data Management
- Computer Operations
- Applications Development And Support

2.5.1 DATABASE ENGINEERING

Databases were once described as collections of files, with files being collections of records which contained items (fields) of information. If you wanted to find a specific record quickly, you had to have separate 'key' files with the keys pointing to related records. Databases have now evolved into massive tables containing columns (items) of information arranged in rows (records) of informational items. Specific information is extracted through the use of elaborate queries that are programming languages unto themselves. Databases no longer embrace just text but images and data in pictorial forms that translate collectively into trillions of bits (1 or 0) of information. Planning for database expansions and protecting data from hardware and software corruption are vital functions performed by database engineers dedicated fulltime to their profession. The Database Architect is responsible for this function, assisted by the Database Administrator.

2.5.2 DATA MANAGEMENT

Databases require routine maintenance such as enlarging table sizes and adding new columns of information. These functions must be done precisely to avoid the risk of data corruption. Data management for the GIS (Geographic Information Systems) is performed by the Sr. GIS Analyst – Systems Administration.

ORGANIZATION

2.5.3 COMPUTER OPERATIONS

In earlier decades, computer rooms were generally staffed 24 hours per day to ensure that all equipment was running properly, that jobs from large printers were being prepared for dissemination, and that the environment was sufficiently cool to offset the heat dissipated by the large mainframe computers. Today, the city's computer room looks and feels much the same, except that the three or four large mainframe boxes have been replaced by racks of over a hundred server-configured computers running simultaneously. There are less print jobs for the staff to prepare because so much information is now gleaned by users directly through query and reporting software that accesses databases directly. Staff performing these duties consists of a supervisor and sufficient computer systems technicians to cover all shifts, 24 hour per day, seven days per week. Some computer rooms today are maintained in a "darkened" mode, meaning they don't have computer operations present in a dedicated manner but have staff verifying proper operation remotely and/or as a collateral duty. This is a future goal, made possible by progress and confidence in monitoring equipment and software, toward which I.T. will gradually progress.

2.5.4 APPLICATIONS DEVELOPMENT & SUPPORT

Unlike the other, behind-the-scenes aspects of Applications Services, this is the one most involving interface with our user community. No I.T. applications project is undertaken at the city without including user input from planning through final testing and implementation.

2.5.4.1.1 BUSINESS APPLICATIONS

This group handles the majority of the I.T. developmental functions, including systems analysis and programming, as well as interfacing with various I.T.-built and vendor-supplied application components. The group is guided by an I.T. Systems Coordinator and staffed with information systems coordinators, systems analysts, and programmers. Because the bulk of I.T.'s computer programming is now supplied by external vendors, the majority of this group's activities are concerned with interfacing and testing.

ORGANIZATION

2.5.4.2 INTERNET/INTRANET/GIS APPLICATIONS

Included in this group's application maintenance responsibilities are less traditional I.T. components, specifically the external Internet, the city's internal Intranet, and the GIS (Geographic Information System) application.

2.5.4.2.1 INTERNET/INTRANET

Staff dedicated to maintaining the city's Internet and Intranet systems consists of systems analysts, Internet developer/analysts, and an information systems coordinator.

2.5.4.2.2 GIS

The GIS (Geographic Information System) software externally-supplied by ESRI (Environmental Systems Research Institute) has become virtually a national standard for allowing custom maps to be produced for local governments. City staff has worked extensively to interface it with aerial Las Vegas Valley photos and political jurisdiction boundaries, as well as digitized layers of objects from fire hydrants to street lights. A close cooperation has developed with Clark County and other local government entities in how the data for this application is maintained, to the benefit of all. Serving I.T. in this capacity are GIS programmers, analysts, and technicians.

ORGANIZATION

2.5.5 APPLICATIONS DEVELOPMENT & SUPPORT

Unlike the other, behind-the-scenes aspects of Applications Services, this is the one most involving interface with our user community. No I.T. applications project is undertaken at the city without including user input from planning through final testing and implementation.

2.5.5.1 BUSINESS APPLICATIONS

This group handles the majority of the I.T. developmental functions, including systems analysis and programming, as well as interfacing with various I.T.-built and vendor-supplied application components. The group is guided by an I.T. Systems Coordinator and staffed with information systems coordinators, systems analysts, and programmers. Because the bulk of I.T.'s computer programming is now supplied by external vendors, the majority of this group's activities are concerned with interfacing and testing.

2.5.5.2 INTERNET/INTRANET/GIS APPLICATIONS

Included in this group's application maintenance responsibilities are less traditional I.T. components, specifically the external Internet, the city's internal Intranet, and the GIS (Geographic Information System) application.

2.5.5.2.1 INTERNET/INTRANET

Staff dedicated to maintaining the city's Internet and Intranet systems consists of systems analysts, Internet developer/analysts, and an information systems coordinator.

ORGANIZATION

2.5.5.2.2 GIS

GIS (Geographic Information Systems) software, externally-supplied by ESRI (Environmental Systems Research Institute), has become virtually a national standard for allowing custom maps to be produced for local governments. It has been employed extensively by the city to interface with aerial Las Vegas Valley photos and political jurisdiction boundaries, as well as digitized layers of objects from fire hydrants to street lights. A close cooperation has developed with Clark County and other local government entities in how the data for this application is maintained, to the benefit of all. Serving I.T. in this capacity are GIS programmers, analysts, and technicians.

2.5.6 MANAGEMENT ANALYSIS

Many projects require the ability to perform complex analysis and produce sophisticated reports, charts, graphs, etc. that I.T. management can use to show a potential application's merits or possible non-fit to departmental managers, enterprise managers, or possibly to other entities in the Las Vegas Valley. One management analyst, highly-skilled in information presentation, currently serves in this capacity.

ORGANIZATION

2.6 CLIENT RELATIONSHIP SERVICES

This is the liaison division within I.T. responsible for winning departments and influencing users. Primary functions include business analysis, project management, media services, quality assurance, technical documentation, and application testing and training.

2.6.1 BUSINESS ANALYSIS

This group is comprised of I.T. business analysts, who interact directly with the user community to learn their businesses to the extent that automation proposals and enhancements are efficient and thorough and that computerization concepts, as they pertain to the specific business involved, are explained and understood fully. This practice of dedicating I.T. staff to learn user business processes is now common within many organizations – even to the point of physically basing business analysts within user locations if the application is sufficiently large.

2.6.2 PROJECT MANAGEMENT

This is the true heart of the Client Relationship Division. Project Management, working with user representatives, helps guide I.T.'s developmental staff, as well as that of COTS (Commercial Off-The-Shelf) providers, in constructing and custom-implementing application systems for city departments. This group consists of I.T. project coordinators, certified, or in the process of being certified, by the Project Management Institute (PMI), a national organization sponsoring training and certification programs for project managers. Project Management staffers coordinate projects from planning through implementation phases, arranging meetings, setting milestones, and generally ensuring that necessary interaction among parties takes place to ensure project completion within established budget and time constraints.

ORGANIZATION

2.6.3 MEDIA SERVICES

Media Services is comprised of Graphic Arts, Reproduction, and Mailroom components. This group is self supporting, charging city departments for products and services provided in an amount to offset labor and material costs.

2.6.3.1 GRAPHIC ARTS

Having Graphic Arts be part of I.T. may not be traditional, but it makes a lot of sense when you consider that today the majority of the original art work produced by this group is computer created, and the reproduction and dissemination of graphics output is now done by computer-controlled means. Group staffing is furnished by graphic artists, graphic illustrators, graphic services technicians, and graphic equipment operators in various grades depending upon seniority.

2.6.3.2 REPRODUCTION

This function is responsible for volume reproduction orders for city departments from products produced by Graphic Arts and/or other departmental contributors. Staffing is provided by a graphic equipment operator, backed up by Graphic Arts staff members in a collateral capacity.

2.6.3.3 MAILROOM

They take the mail to the Post Office, right? Well, it's a little more involved than that. The Mailroom *prepares* mail before it's taken to the post office, so that it arrives ready for distribution to the next step in the postal process. It's very handy having a 'local' post office on site, from which we can not only buy stamps but also purchase priority and proof-of-delivery mail services.

ORGANIZATION

2.6.4 QUALITY ASSURANCE/QUALITY CONTROL

This function reviews project-related documents for completeness and consistency and assists in drafting policy and procedure documents. The quality assurance administrator in this role also coordinates the various change control committees that review changes to application systems before approval for implementation into production instances.

2.6.5 TECHNICAL DOCUMENTATION

Technical documentation embraces drafting policies, procedures, guidelines, and technical and user documentation for applications. The job requires a college degree or equivalent experience and demands excellent writing skills, including content organization and grammatical correctness. This is a new position in I.T. that will no doubt provide benefit by now making a dedicated staff member available for this all-important project component that was previously handled as a collateral duty.

2.6.6 QUALITY ASSURANCE TESTING/TRAINING

This new I.T. function will be responsible for coordinating application testing activities for thoroughness and consistency. Assisting in this process will be new interactive testing software for functional and load testing, for which the quality assurance coordinator will be the administrator.

ORGANIZATION

2.6.7 TECHNICAL DOCUMENTATION

Technical documentation embraces drafting policies, procedures, guidelines, and technical and user documentation for applications. The job requires a college degree or equivalent experience and demands excellent writing skills, including content organization and grammatical correctness. This is a new position in I.T. that will no doubt provide benefit by now making a dedicated staff member available for this all-important project component that was previously handled as a collateral duty.

2.6.8 QUALITY ASSURANCE TESTING/TRAINING

This new I.T. function will be responsible for coordinating application testing activities for thoroughness and consistency. Assisting in this process will be new interactive testing software for functional and load testing, for which the quality assurance coordinator will be the administrator.

ORGANIZATION

2.7 SYSTEMS INFRASTRUCTURE MANAGEMENT

This division of I.T. functions at the systems administration and engineering levels and provides support for the city's local and remotely-located personal computer networks and devices. Personal computer equipment supported includes desktops, laptops, PDAs (Personal Digital Assistants), and related devices such as printers and scanners.

2.1.1 SYSTEMS ENGINEERING

Systems administration specialists support the city's systems engineering work, which includes administration of the over 100 servers located in the main computer room and at the backup site located 10 miles from the primary facility, as well as the attendant systems software. Making this work together smoothly is an incredibly complex and mind-consuming affair.

2.1.2 COMMUNICATIONS ENGINEERING & ADMINISTRATION

This staff ensures proper installation and operation of new and existing network lines (including those for wired local telephones and optical fiber data communications) by utilizing their years of experience together with adequate testing procedures. The group includes senior communications technicians, a serior data communications technician and an office specialist II.

2.1.3 DESKTOP SYSTEMS SUPPORT

Desktop Systems Support is self-sustaining, with a chargeback to each department annually, based on the proportionate use. They use the latest and best Microsoft tools, including SMS (Systems Management Server) for dispensing software updates and patches to all users via the network. These professional maintain certifications in their particular areas of endeavor in an effort to keep up with the latest techniques and equipment.

ORGANIZATION

2.1.3.1 DESKTOP APPLICATIONS SUPPORT

When desktop computer problems warrant an onsite response, this group of microcomputer specialists answers the call. Friendly and courteous, these experts always dispense service with a smile. However, because the systems fail so rarely, users see them only occasionally. Computer systems technicians also provide physical placement and relocation of desktop computer equipment as needed.

2.1.3.2 I.T. SUPPORT DESK

Calls that were, in the past, handled by helpdesk technicians are now channeled directly to the same group of microcomputer specialists performing onsite calls. This effectively removes the middle person, and the more direct contact between users and the most knowledgeable staff enables problems to be resolved more quickly. All problems are logged, described, and properly closed so that accurate statistics are always available. If necessary, these micro specialists can take control of networked user computers remotely and maneuver the cursor themselves, while reviewing the particular difficulty. This often makes onsite trips unnecessary. The I.T. Support Desk phone number is posted on the I.D. tag of each desktop and laptop computer.

2.7.4 NETWORK AND INTERNET/INTRANET ENGINEERING

The city's local and wide area networks are managed by this group, consisting of systems administration specialists certified in network engineering. The wide area network now comprises over 50 remote locations.

SECTION 3 - KEY I.T. GOVERNANCE FUNCTIONS

FEATURED IN THIS SECTION

3.1 APPLICATIONS MANAGEMENT
3.2 APPLICATIONS TESTING
3.3 ASSET MANAGEMENT
3.4 BUDGET AUTHORITY
3.5 BUDGET PLANNING AND PROCESS
3.6 BUSINESS ANALYSIS
3.7 CAPACITY PLANNING
3.8 CHANGE MANAGEMENT.
3.9 COMMUNICATIONS MANAGEMENT
3.10 COMPUTER OPERATIONS
3.11 COST ALLOCATION
3.12 DATA MANAGEMENT
3.13 DESKTOP SUPPORT
3.14 eGOVERNMENT PLANNING AND ADMINISTRATION
3.15 NETWORK MANAGEMENT
3.16 PORTFOLIO MANAGEMENT
3.17 PROJECT MANAGEMENT
3.18 QUALITY ASSURANCE
3.19 REFERENCE
3.20 RESOURCE MANAGEMENT
3.21 SECURITY AND CONTINGENCY PLANNING
3.22 SERVICE LEVEL AGREEMENTS (SLAs)
3.23 STRATEGIC PLANNING
3.24 SYSTEMS ADMINISTRATION
3.25 TECHNICAL ARCHITECTURE

KEY I.T. GOVERNANCE FUNCTIONS

3.1 APPLICATIONS MANAGEMENT

FEATURED IN THIS SECTION

3.1.1 DEFINITION

3.1.2 OVERVIEW

3.1.3 PROGRAMMING LANGUAGES

3.1.4 SOFTWARE TOOLS

3.1.5 PROJECT LIFECYCLE

3.1.6 DOCUMENTING APPLICATIONS MANAGEMENT

3.1.7 GEOGRAPHIC INFORMATION SYSTEM (GIS)

APPLICATIONS MANAGEMENT

3.1.1 DEFINITION

Applications Management involves the creation, acquisition, and support of computer programs designed to fulfill a specific set of purposes for computer users within an organization. These programs may be developed inhouse or acquired from software vendors.

3.1.2 OVERVIEW

The applications management function is performed by the Applications Services Division of I.T. The primary objectives of this division are to provide the city with:

- Applications
- Systems consultation with departmental users
- Software and systems integration
- "Point" solutions implementation
- Applications operation and support

To achieve these objectives, the division is responsible for, or involved in:

- Identifying software needs within the city's departments
- Performing the necessary analysis and providing reasonable solutions
- Developing, or acquiring through purchase, the needed software
- Administering and maintaining the application software

Primary applications sections within the division are:

- Oracle (Finance/Human Resources)
- Client/Server
- GIS (Geographic Information Systems)
- Web (Internet and Intranet)
- Legacy

A sample of a GIS Internet application web page provided to citizens is shown in the appendix. This application accepts input of an address over the Internet and displays neighborhood air views from multiple heights through a zoom control feature. Also, shown as a sample in the appendix, is a homepage view from the Intranet, which is provided for employees to keep in touch with management, get weather reports, buy and sell items, etc.

APPLICATIONS MANAGEMENT

How is the decision to go inhouse or purchase a solution from a vendor made? Often, a user will have learned about a particular product that fits their needs and will come to I.T. to determine if it can work alongside existing systems. Obviously, systems already built can be put into service more quickly than inhouse developed software, even if significant time has to be spent on integration and testing. Some Purchased Software Evaluation Guidelines are provided on the Intranet web site to provide assistance in making this determination and also copied in the policy/procedure section of this document.

Some of the applications supported as of April, 2005 are listed below:

- Accounts Payable
- Budget
- Building and Safety
- Business License
- City Attorney
- City Internet Web Site
- Detention and Enforcement
- Document imaging
- Enterprise Intranet Web Site
- Fire Incident Reporting
- Fixed Assets and Accounts Receivable
- General Ledger
- Human Resources
- Interactive Voice Response (IVR)
- Inventory
- Leisure Services
- Municipal Courts
- P-Cards (for purchases)
- Payroll
- Planning
- Public Works
- Purchasing and Contracts
- Sewer Billing
- Time and Attendance
- Workers' Compensation
- Workflow

Many of the legacy applications that were in use at the city are being replaced by a comprehensive, integrated system provided by Hansen Information Technologies over a four-year span. The functions served include Business Services, Public Works, Planning and Development, and Building and Safety. The new applications are more user-friendly and permit reports to be generated more readily.

The information provided by reports can be the basis for critical management decisions; therefore it is important that steps are taken to minimize errors as much as possible. A Report Request Policy and companion Report Request Form Procedure were created to help ensure that reports are being created on a sound basis and have had their intended functionality and purpose reviewed by others before being placed into production.

APPLICATIONS MANAGEMENT

3.1.3 PROGRAMMING LANGUAGES

Programming languages allow direction to be given to computers. This is done using symbols that we humans understand (source code), and then having this converted by programming language compilers into strings of 0's and 1's (object code) that cause computers to function. A list of programming languages currently in use, with related application areas, is shown below. The list includes three languages from GIS-provider ESRI (Environmental Systems Research Institute).

Programming Language	Applications Area	User Group
ASP	Web-based Apps – Internet Intranet	 Citizens City Employees
COBOL74	Legacy applications	Municipal Courts, Detention, Building and Safety, Business Services
Delphi	Cash Receipting Timecard Senior Law Project	Finance Payroll, City Employees Leisure Services
SQL	Database Query Tool	I.T. Staff
Visual Basic	Plans Viewer GIS (Geographic Information Systems)	Planning I.T. GIS Staff
VBA (Visual Basic for Applications)	E.I.S. (Executive Information System)	City Employees
ESRI Avenue (Scripting tool to automate tasks)	GIS	I.T. GIS Staff
ESRI AML (Arc Macro Language)	GIS Data Maintenance	I.T. GIS Staff
ESRI ArcXML (Spatial version of XML – eXtensible Markup Language)	GIS Web-based Apps	Citizens, City Employees

APPLICATIONS MANAGEMENT

Source code must be managed properly to ensure its accuracy; and having effective source code management and version control policies in place are key steps in achieving this goal.

There are many more application areas being serviced by I.T. than shown in the previous diagram. However, the software for these areas is being provided by third-party vendors, the major ones being:

- Oracle (Finance, Human Resources)
- Hansen Information Technologies (Permitting, Land Use, Business Licensing, Code Enforcement, Asset Management, Customer Service)
- Active Community Solutions (Class – for Leisure Services)

3.1.4 SOFTWARE TOOLS

A number of software tools are used by applications staff to assist in software development, version control, testing, and tracking client requests and problems:

- (HEAT – Help Expert Automation Tool) – used for logging client requests
- Crystal Reports – for generating reports from a database
- Mercury Interactive software - for testing and for defect tracking
- Microsoft Office Suite – contains familiar Word, Excel, and PowerPoint applications
- Oracle Form Builder – allows online forms to be developed to accept data into Oracle databases
- Oracle Development Tool (TOAD) - online query tool for viewing tables, indexes, etc.
- Oracle Report Builder – allows reports to be generated from Oracle databases
- Version Control System (PVCS) – assigns unique numbers and dates/times to software versions to differentiate them from one another

3.1.5 PROJECT LIFE CYCLE

There are basic stages in software development that separate it into its most logical components:

- Planning
- Requirements Definition
- Functional Design
- System Design
- Programming
- Integration and Testing
- Installation and Acceptance
- Maintenance (on-going)

APPLICATIONS MANAGEMENT

The need for stages such as planning, design, programming, testing, and maintenance would be obvious to even those unfamiliar with I.T. However, to actually carry out quality software development from beginning to end, many more steps must be followed. The process below was developed by Applications Division staff after reviewing methodologies used by others for this purpose and revising the steps through use.

1. A client requests a new application or modification to an existing one.
2. A HEAT call is created by the Help Desk or the project lead.
3. If the project team consists of more than two people, a Scope of Work document is written.
4. A software development methodology is chosen.
5. A design is developed.
6. Approval is obtained from the DBA (Database Administrator).
7. Approval is obtained from appropriate Systems Infrastructure Division staff.l.
8. Client Support approval is obtained.
9. The software is developed.
10. The software is tested.
11. Additional release iterations may be accomplished by returning to step 5, involving design development.
12. When the final release is ready for implementation, all required artifacts are checked into PVCS (the version control system).
13. The project lead fills out the appropriate approval form and emails it to his/her supervisor.
14. The supervisor performs necessary QA.
15. The supervisor promotes the artifacts in PVCS to the "Approval" promotion group.
16. If supervisory approval is all that is required:
    a. The supervisor approves the request.
    b. The supervisor informs the project lead that the request was approved.
17. If managerial approval is all that is required:
    a. The supervisor passes the "Request for Approval" document to the manager.
    b. The manager reviews the documentation.
    c. The manager approves the request.
    d. The supervisor informs the project lead.
18. If ITCCC (I.T. Configuration Control Committee) approval is required:
    a. The supervisor informs ITCCC support of the request to implement a project.
    b. The project lead submits to the ITCCC the filled out ITCCC Request Form and supporting documentation, particularly describing testing.

(Continued)

APPLICATIONS MANAGEMENT

c. ITCCC reviews the project and votes on the motion to implement. (At the meeting, the project lead makes preparations and presents the project to the committee. This may include any background information, scope of work, testing procedure and results, implementation plan, etc.)

19 If this is a new application, the project lead informs the Help Desk of the new application and provides them with any information that they require.

20. The supervisor promotes the software to the "Production" promotion group.
21. The supervisor forwards the request to the Help Desk, asking to implement the software.
22. The Help Desk creates a new Heat Call, copies and pastes the information in the request, attaches the approval document, and assigns it to Systems or Client Support.
23. Software is installed from PVCS.
24. Systems/Client Support informs project lead and supervisor when the software has been installed.
25. The project lead follows up with users to verify that the software is working per requirements.
26. The project is completed.

The Software Development Life Cycle Policy is discussed in more detail in the policy/procedure section.

3.1.6 DOCUMENTING APPLICATIONS MANAGEMENT

Various documents are useful in recording many of the details associated with an applications project. The more this process is followed, the less likely errors will occur because those associated with the project are then viewing things in a more similar manner. Documentation can help to pinpoint problems more reliably since now everything is not being recalled from memory. Reviewing previous projects before beginning new ones allows documentation to prevent problems from occurring again. Depending upon the size of the project and whether it is developed inhouse or purchased, some of these documents may not need to be created. For example, it may not be necessary to develop a data model and a data dictionary if the application is provided by a supplier.

APPLICATIONS MANAGEMENT

Some of the documents in current use are:

- Assumptions and Constraints
- Cost Estimates
- Data Model
- Data Dictionary
- Issue / Problem Log
- Project Log
- Problem / Purpose Definition
- Process Flowchart
- Requirements Documents
- Risk Analysis
- Roles and Responsibility Levels
- Stakeholders and Contacts
- Test Scripts
- Time Line / Gantt Chart

3.1.7 GEOGRAPHIC INFORMATION SYSTEM (GIS)

The city now has a sophisticated GIS (Geographic Information System) that it began installing in 1988. Over the years, all of the basic data has been input, and now the never-ending task is to keep it up to date so that information can be obtained from it quickly and with confidence. The system allows any data associated with a valid parcel number or address to be located on a computer-generated map. The city maintains a close cooperative association with Clark County so that GIS data changes are updated together and are reflected on maps produced by either entity. The process involved with updating the database is complex and involved due to the complex nature of the system itself. These update procedures are meticulously documented and followed to avoid errors.

Information regarding specific items is stored in layers in the database and can be combined, often with other layers, to generate unique maps for use by staff and citizens. Examples of layers are traffic lights, sewer line locations, school locations, traffic accidents, metropolitan police crime data, etc. A recent technique that has shown merit is that of "trending," or viewing multiple map images over time, and thus being able to anticipate a need or a consequence of a scheduled action. For example it might be useful to combine the accident layer with the traffic light layer over time to see if certain areas without lights need them or if intersections with lights might need to have them retimed. An example of a GIS application much used by citizens is the address/parcel locater demonstrated at the end of this document.

KEY I.T. GOVERNANCE FUNCTIONS

3.2 APPLICATIONS TESTING

FEATURED IN THIS SECTION

3.2.1 DEFINITION

3.2.2 OVERVIEW

3.2.3 TESTING TYPES

APPLICATIONS TESTING

3.2.1 DEFINITION

Applications Testing refers to the procedures associated with the specific types of software testing involving programmers and application users.

3.2.2 OVERVIEW

As of 2005, I.T. is being trained in, and practicing with, the use of tools to assist in managing software testing. These tools offer a number of services, among them:

- Automated test management - including defining test requirements, creating test cases, combining test cases into test sets, tracking application defects, and working with other users through a collaboration module
- Creating automated scripts for functional testing in a standard Windows environment that can be used repeatedly, helping to provide more consistent results
- Creating automated scripts for load and stress testing

Details for carrying out software testing are described in I.T.'s Software Testing Policy and Software Testing Procedure.

3.2.3 TESTING TYPES

Specific types of software testing include:

- **Usability Testing** – measuring how well people can actually use something (such as a web page, a computer interface, a document, or a device) for its intended purpose. If users, or test subjects, have difficulty understanding instructions, manipulating parts, or interpreting feedback, then the developers must go back to the drawing board, improve the design, and perform the usability test again.
- **Data Integrity** – verifying that the data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
- **Unit Testing** – isolating each part of the program and show that the individual parts are correct.
- **Regression testing** – re-running of previously-run tests and checking whether previously-fixed faults have reemerged.
- **Integration testing** – combining all of the parts of an application to determine if they function together correctly. This test is usually performed after unit and functional testing. This type of testing is especially relevant to client/server and distributed systems

(Continued)

APPLICATIONS TESTING

- **System Testing** – testing the combination of applications used in a business process together.
- **Compatibility Testing** – testing a product's capability to interface with other software and hardware.
- **Stress Testing** – combining an availability test and a throughput test. Availability testing involves testing the reliability of the network, database processor, memory, etc. This involves testing the capability to have the support for critical data required by the applications to be up and running in minimum standard conditions. All of the architectural components that need to be available are also ensured to be present and functional. Throughput testing is used to test the load-bearing capacity of the system and to measure the response time and throughput of the various system components.
- **Acceptance Testing** – user testing of the system and, based on the results, either granting or refusing acceptance of the software system being delivered.
- **Sanity Test Scripts** – briefly running through the main functionality of a computer program or other product to provide a measure of confidence that the system works as expected prior to a more exhaustive round of testing.
- **Installation Testing** – installing a tested copy of the software onto a copy of the production environment. This test confirms that the application can be installed without expected or unexpected events causing a loss of data or functionality of other system components.
- **Recovery Testing** – testing to confirm that the program recovers from expected and unexpected events without loss of data or functionality. Events can include shortage of disk space, unexpected loss of communications, or loss of power conditions.

KEY I.T. GOVERNANCE FUNCTIONS

3.3 ASSET MANAGEMENT

FEATURED IN THIS SECTION

3.3.1. DEFINITION

3.3.2 ASSET LIFE CYCLE

3.3.3 ASSET RESPONSIBILITY

3.3.4 ASSET CONTROL

3.3.5 ASSET MANAGEMENT

ASSET MANAGEMENT

3.3.1 DEFINITION

Asset – An item of value.
Asset Management – Guiding the acquisition, use, and disposal of assets, and managing the related costs and risks over the entire asset life cycle, from planning through disposal.

3.3.2 ASSET LIFE CYCLE

Generally, four phases are described to cover the 'life' of an asset:
(1) Planning; (2) Acquisition; (3) Operation and Maintenance; (4) Disposal.

(1) Planning for asset acquisition involves approval by management of the identification of a requirement or need. At the city, this can occur at any time during the year. Once I.T. has identified new asset requirements for the coming July 1 – June 30 Fiscal Year, they are submitted for approval by Finance and city management as part of the budget cycle beginning in December (see Budget Planning and Process). These 'budgeted' items are now ready for the acquisition phase. Assets costing more than $25,000 require additional approval by the elected City Council.

(1) Acquisition involves purchasing the item. Items that are approved for purchase during the budget cycle in December through March can be purchased after the following June 30, which marks the beginning of the city's Fiscal Year Calendar. If needed, non-budgeted items can be acquired at any time provided that necessary funding and approvals can be secured. The Purchasing Section of the Department of Finance and Business Services (Finance) is responsible for advertising, securing bids, and contacting vendors. Purchases must be approved at the director or managerial level (See Budget Authority.)

(3) Operation and Maintenance is where the asset is used for its intended purpose. During this time the asset may be repaired or improved in some way, however, it still carries the same I.D. tag as when it was first put into service. Computerized records are maintained by Finance of all assets valued at greater than $5000. I.T. keeps separate database files of equipment based on functionality, for example, server records are maintained by the the Systems Engineering group and desktop-related equipment is inventoried by the Applications Support group.

(4) Disposal occurs when the asset has reached the end of its useful life or the need for which it was acquired is no longer present. If no alternative use (for example, as a backup) can be found, the asset is then marked for salvage and removed from the database records.

3.3.3 ASSET RESPONSIBILITY

Obviously it is everyone's responsibility to care for assets properly; but it is the managers' responsibility to ensure that this happens. In I.T., our managers are involved in all four asset management phases in both direct and guiding roles. This is particularly true in the planning phase, in an effort to stay within budget constraints.

3.3.4 ASSET CONTROL

Control of an asset is said to occur when an organizational entity has the capacity to enjoy the benefits of the asset, either present or planned, and can permit or deny the use of the asset to others according to what that entity believes to be in the best interests of the organization as a whole. I.T. controls a myriad of computer hardware, software, and services for just such a purpose – to service the City of Las Vegas and its citizens to the maximum extent possible.

Because this material is used collectively to provide benefit to those being served, I.T. must control what is purchased for use by departments from outside vendors in order for compatibility of all products to be assured. All hardware is acquired by I.T., and issued to to client departments via Service Level Agreements (SLAs). All new department-specific hardware and software running on client PCs must be tested by the I.T. Desktop Applications Support Group and then approved for use by the Configuration Control Committee before implementation is allowed to occur (see Change Management and Software Change Control Policy). Other pertinent matters regarding hardware and software control are covered in the microcomputer hardware and software policies

3.3.5 ASSET MANAGEMENT

Effective I.T. asset management allows those providing direction to address priorities and objectives. Compliance with legislated data security and privacy issues is affected by how assets are controlled and used (see Web Site Privacy Policy). I.T. must know what assets it owns, who is using them, and where they are to demonstrate that its data is properly secured and that I.T. has met its fiduciary responsibilities.

ASSET MANAGEMENT

Asset management programs need to demonstrate business value to be successful. I.T.'s desktop support services, in which city departments are charged a fixed price annually per desktop, is an example of this practice. This program uses asset management to provide business value through:

- Increased functionality
- Appropriately managing the environment
- Cost savings and cost avoidance
- Risk Avoidance

I.T.'s Applications Services and Client Relationship Services divisions both realize business value by working with departmental clients to link I.T. and business objectives and to prioritize activities and expenditures.

I.T. personnel are charged with caring for the assets that are associated with their job responsibilities on a day-to-day basis. However, it is I.T. managers who are tasked with ensuring that assets are planned for, acquired, operated and maintained, and disposed of properly in accordance with asset life cycle principles.

While not always practical, whenever possible assets should be shared - particularly those that are used infrequently. An example would be I.T.'s policy of sharing the audio/visual equipment used in making meeting room presentations. (See Audio/Visual Equipment Policy/Procedure.)

Gartner reported in November, 2004 that organizations are recognizing more and more that asset management "adds value and lessens risk." "IT asset management is receiving more attention as businesses continue to face cost controls and increased asset regulatory requirements." Gartner recommends that the best way to implement sound asset management programs is to "combine people, processes and tools."

KEY I.T. GOVERNANCE FUNCTIONS

3.4 BUDGET AUTHORITY

FEATURED IN THIS SECTION

3.4.1. DEFINITION

3.4.2 OVERVIEW

BUDGET AUTHORITY

3.4.1 DEFINITION

Budget Authority involves the authority to enter into obligations that normally result in the outlay of funds. The main forms of budget authority are appropriations, borrowing authority, and contract authority.

3.4.2 OVERVIEW

As part of normal operations, non-managerial I.T. staff members are not authorized to appropriate funds for hardware and software purchases and to enter into contracts for services (e.g., for maintenance), leases (e.g., of hardware and software), and rentals (e.g., of equipment or space). The persons engaged in these activities are limited to the Director and the division managers. Key technical staff members recommend the appropriation of funds, but managers or above must give final approval. Borrowing authority is reserved for staff in the Department of Finance and Business Services.

I.T. budget requests at the City of Las Vegas are governed by the anticipated period of use of the service or item (one year, multiyear, or less than one year), by the specificity of the amount required in conjunction with the amount available, and the need to consider the appropriate Fiscal Year (July 1 through June 30) boundary during which the request is needed (current, next, current plus next, etc.)

Although only department directors and managers can approve purchases directly, all employees can participate in budget planning and the budget process by making recommendations and documenting how the proposed purchases can provide benefit to I.T. and the enterprise.

KEY I.T. GOVERNANCE FUNCTIONS

3.5 BUDGET PLANNING AND PROCESS

FEATURED IN THIS SECTION

3.5.1 DEFINITION

3.5.2 OVERVIEW

3.5.3 BUDGET CALENDAR

3.5.4 SAMPLE BUDGET PREPARATION WORKSHEET

BUDGET PLANNING AND PROCESS

3.5.1 DEFINITION

Budget Planning is a program or method worked out beforehand for the assigning of indirect, general, and administrative costs for activities, functions, assets, or outputs involved in accomplishing organization objectives. The Budget Process involves the steps for preparing the budget through final approval.

3.5.2 OVERVIEW

Budget planning within I.T. occurs throughout the year as new hardware and software needs are noted and documented by staff and management. An early official step is creation of the coming Fiscal Year's budget preparation manuals for the operating and the capital budgets by the Budget and Finance Division. This occurs during October and November. While a 70+ page document is imposing to look at, it is not as difficult to create as it may appear because the previous year's copy is used as a base. These comprehensive guides cover every aspect of budget preparation, including all of the steps necessary when applying for grant funding. Next, a budget kickoff meeting is held between management and departmental representatives in early December. At this time, I.T., along with other city departments, begins the process of internal and external meetings that will lead to preparation of an initial budget by February for the approaching Fiscal Year that will begin in July.

Ideally, every employee plays a role in budgeting – through formulation, preparation, evaluation, execution or administration. This is particularly true in I.T. because of the high degree of technical knowledge needed. Ultimately, each department director through the City Manager is accountable to the City Council for the performance of departmental personnel in meeting specific objectives within allocated resource limits. At the department level, budget authority is limited to directors and division managers. Once adopted, the final budget provides the legal basis for the expenditure of funds in accordance with the City Council's priorities, established policies, and strategic planning.

BUDGET PLANNING AND PROCESS

Development of a budget is a political and managerial process that has financial and technical dimensions. Budget preparation allows departments the opportunity to reassess goals and objectives and the means for accomplishing them. Employees are encouraged to think in terms of strategic planning, diligent preparation, thorough review, and informative presentation. The city's budget process is intended to be a meaningful planning and teamwork exercise for departments as well as a means to develop the budget into a document that will provide the City Council with a basis for making policy decisions. Budget proposals authored by staff have the potential to be reviewed by the Mayor, City Council, City Manager, and citizens to ensure that the highest priorities are being managed with the most prudent financial solutions. With the provision of reliable information regarding the relative importance of city programs, the City Council and staff will be in the best position to analyze alternative courses of action in terms of how the available resources can be used to achieve the maximum public benefit.

Departments are required to submit a base budget request each year not to exceed predefined expenditure targets to ensure a balanced financial plan. The non-labor expenditure targets are based upon previous Fiscal Year budgets adjusted for known changes in programs blended with initial guidance provided by the City Manager's Office. Departments may also submit an Expanded Budget Request that is limited to mandated program expansion or new programs having new or expanded revenue sources to offset the increase in expenditures.

Meetings between the City Manager's Office, the Department of Finance and Business Services' Budget and Finance Division staff and departments begin in February. The Citizens' Priority Advisory Committee (CPAC) is requested to submit a report of its review to the City Council at the Public Budget Hearing scheduled in Mid-May.

A Budget Calendar is disseminated to all departments to use as a guide in adequately preparing their budgets. The establishment of a budget calendar, which is partially determined by Nevada State law, is necessary to properly schedule completion dates to ensure a prompt and efficient budget process. Following is an outline of a typical Fiscal Year Planning Calendar.

BUDGET PLANNING AND PROCESS

3.5.3 BUDGET CALENDAR

BUDGET CALENDAR

DATE	ACTION TO BE TAKEN
Early December	Department Budget Kickoff Meeting – Operating and Capital Budgets
February 1	Budget requests due from departments to Budget and Finance Division, as required by Municipal Code 4.08.010
Late February	Budget and Finance meets with City Manager's Office to review departmental submissions and budget recommendations
Early March	Publish notice for City Council Budget Workshop
Mid-March	City Council Budget Workshop
April 15	Tentative Budget due to Nevada Department of Taxation, Clark County Clerk, and Las Vegas City Clerk
Mid-April	Tentative Budget/Capital Improvement Plan submitted to Citizens' Priority Advisory Committee
Early May	Publish notice for hearing on Tentative Budget
Mid-May	City Council holds public hearing on Tentative Budget and indicates changes to be included in the Final Budget. Report on Citizens' Priority Advisory Committee's review of Tentative Budget submitted to City Council. City Council adopts Final Budget and Five-Year Capital Improvement Plan with the changes indicated.
June 1	Final Budget due to Nevada Department of Taxation, Clark County Clerk, and Las Vegas City Clerk
Early June	Final Budget review meetings with all Departments; distribution of final budget schedules
July 1	Beginning of new Fiscal Year

BUDGET PLANNING AND PROCESS

3.5.4 SAMPLE BUDGET PREPARATION WORKSHEET

With the process being continually improved year after year, the various sections of the budget preparation manuals have come to request considerable information but, for the most part, only what is necessary. To convey an idea of the sophistication that has evolved, a sample form, the "Instructions for Schedule 2 New or Expanded Program Analysis" with the associated questionnaire, is shown in the Appendix.

KEY I.T. GOVERNANCE FUNCTIONS

3.6 BUSINESS ANALYSIS

FEATURED IN THIS SECTION

3.6.1 DEFINITION

3.6.2 OVERVIEW

BUSINESS ANALYSIS

3.6.1 DEFINITION

In I.T., Business Analysis refers to the process carried out in the users' workplace by I.T.-based and loaned-out business analysts to determine the requirements, fit, cost, applicability, and maintainability of computer applications for the benefit of users and the enterprise.

3.6.2 OVERVIEW

I.T. must form a close partnership with enterprise departmental customers. The "I.T." that they see is most often whoever is dispatched by I.T. to look at the project or problem from the customer point of view. Business analysis for I.T., up until the present, has been performed by systems analysts who work in I.T. and only visit the users' work areas for meetings on occasion. Many, if not all, application systems meetings are held in I.T. or other central locations, affording I.T. staff little chance to thoroughly understand users' business needs. If this could be done more adequately, then it is reasonable to assume that I.T. staff could identify computer solutions for users that would be more appropriate and more cost effective. The opposite tack is to have users vying for their own applications, which often run afoul of enterprise network, operating system, database, and hardware standards.

One solution is to dedicate I.T. business analysts to work almost completely in user areas, thereby observing, and identifying with, user needs from their point of view. These specialists would serve more than one user department, and would already be endowed with I.T. knowledge and skills. The additional skill that it is important for them to have is communicating with people in a relaxed and friendly manner.

Approval for business analysis positions is being sought during 2005 in the budget for the following fiscal year. Possibly, funding will be jointly shared by I.T. and among user departments. It may also be advantageous to employ business process modeling tools, which seek to bridge the business/IT divide, by empowering line-of-business analysts to define business processes in a visual modeling environment that is tightly integrated with I.T. process execution.

KEY I.T. GOVERNANCE FUNCTIONS

3.7 CAPACITY PLANNING

FEATURED IN THIS SECTION

3.7.1. DEFINITION

3.7.2 OVERVIEW

CAPACITY PLANNING

3.7.1 DEFINITION

Capacity planning is the process of specifying resource service levels (facilities, equipment and human resources) that best meet current and future operational workloads.

OVERVIEW

During each year's budget planning cycle, I.T. managers and staff look at the past year's resource requirements and usage and attempt to determine what will be needed for the coming year. Not only must expanding capacity to accommodate growing client requirements be considered, but planning for new hardware and software systems must be taken into account. This can be a complex process requiring looking ahead two to five years in the future, depending upon the resource(s) under consideration.

This process can now be done using automated tools that allow current system capacity and workloads to be specified, growth parameters to be input, and then have future loads and capacity requirements extrapolated. While I.T. is currently considering the cost/benefit of acquiring such a tool (e.g. from Mercury Interactive), due diligence continues to be given to capacity planning in the more traditional manner, i.e., using the experience of managerial and technical staff.

KEY I.T. GOVERNANCE FUNCTIONS

3.8 CHANGE MANAGEMENT

FEATURED IN THIS SECTION

3.8.1 DEFINITION

3.8.2 OVERVIEW

3.8.3 I.T. CONFIGURATION CONTROL COMMITTEE

3.8.4 ORACLE CHANGE REVIEW COMMITTEE

3.8.5 HANSEN CHANGE COMMITTEE

3.8.6 CLASS CHANGE COMMITTEE

CHANGE MANAGEMENT

3.8.1 DEFINITION

A change is defined as anything — hardware, software, system components, documents, and so on — introduced into the I.T. environment that may impact the I.T. service level. Change management within the I.T. environment encompasses the policy, rules, procedures, information, activities, roles, authorization levels, and states relating to the creation, updates, approvals, tracking and archiving of change requests and problem reports. Change management generally includes management of the requirements and functional specifications during project development as well as changes to live systems. Changes can be either permanent or temporary. Permanent changes completely replace a current version of a component. Temporary changes are put in place until a permanent change can be implemented or to serve a particular purpose.

3.8.2 OVERVIEW

The primary goal of change management is to provide a mechanism to facilitate configuration management. Configuration management deals with maintaining the hardware, software, and other relevant components of the Department of Information Technologies (I.T.) infrastructure.

Other goals of change management are:

- To protect the I.T. environment from potentially disruptive changes.
- To ensure that all parties affected understand the potential impact of the impending change to their respective environments. Since most systems are heavily interrelated, any change made in one part of a system may impact another. Change management attempts to identify all affected systems and processes before the change is implemented in order to mitigate or eliminate any adverse effects. Change management seeks to notify all affected parties not simply before releasing new versions into the production environment but to provide these parties sufficient time to plan adequately for potential disruption to operations.
- To evaluate, prioritize, monitor, and plan effectively to minimize the impact to the enterprise environment, including its protection from potentially disruptive changes.

The major objective of the change management process is to introduce change into the I.T. environment accurately and with minimal disruption to service. Change management is responsible for changes in technology, systems, applications, hardware, tools, documentation, and processes, as well.

CHANGE MANAGEMENT

Other objectives of change management include:

- Providing a standardized and comprehensive approach to the implementation of changes to the I.T. environment
- Minimizing disruptions to the I.T. environment
- Handling the evaluation and approval process for all change requests promptly and efficiently
- Establishing implementation schedules
- Communicating with those affected by the change
- Monitoring the activities of planning, developing, testing, and implementing changes to the I.T. environment

Change management deals with changes that:

- Affect multiple users
- Could potentially disrupt mission-critical functionality
- Involve hardware (such as servers) or software modifications
- Involve operational and process modifications that affect multiple users
- Involve network modifications

Change management is not about:

- Regularly-scheduled maintenance
- Frequently performed administrative tasks
- Minor service requests such as changing a password

.

Occasionally, it becomes necessary for emergency changes to be made. Emergency changes require implementation as quickly as possible to prevent significant user downtime and the loss of mission functions. In emergency situations, depending on the required urgency of the release, limited testing and release management activities are executed prior to implementation. Emergency releases/updates should be avoided because they pose the greatest risk to the live environment.

Software change control principles are spelled out in a long-standing Software Change Control Policy. As of 2005, I.T. software change control is controlled by four committees, each of which was formed to meet a specific application/system need. The central ITCCC (I.T. Configuration Control Committee) handles infrastructure hardware and software changes. While it is recognized that having one central change control authority may be ideal, the multiple-committee solution has worked most satisfactorily at the city, and no serious problems have resulted over the past six years of its use. The change committees are:

- I.T. Configuration Control Committee (ITCCC)
- Oracle Change Review Committee (for Oracle-based applications)
- Hansen Change Committee (for Hansen-provided applications)
- Class Change Committee (for Leisure Services applications)

CHANGE MANAGEMENT

3.8.3 I.T. CONFIGURATION CONTROL COMMITTEE (ITCCC)

This committee reviews all hardware changes before going live and all software changes that are not directly related to the Oracle, Hansen, or Class applications systems before being put into production. This includes changes to the "standard image" for hardware and software systems that comprise the city's desktop environment. The process of utilizing the committee is explained in more detail in the ITCCC Change Request Procedure. The ITCCC meets once per week or as necessary. E-mail voting is also utilized if time or space constraints are encountered. Committee membership and function are described in the ITCCC Charter in the Appendix.

3.8.4 ORACLE CHANGE REVIEW COMMITTEE

All changes to the Oracle Financial and Human Resources applications systems, whether to test or production instances, are reviewed by this committee. Requests are submitted to a coordinator, e-mailed to committee members, votes are tabulated, and the results disseminated. All committee members, or their designated backups, must vote approval for any change to proceed. The function of the Oracle Change Review Committee is described in more detail in the Oracle Change Review Process document within the Appendix.

3.8.5 HANSEN CHANGE COMMITTEE

Hansen Information Technologies' extensive set of integrated applications serves business services, public works, and building and safety functions. All changes to the Hansen applications systems, whether to test, training, or production environments must be approved by all voting members of this committee, or their designated backups. A coordinator receives the change requests, assigns a unique number to each, forwards the requests to committee members, tallies the votes, then notifies the requestor and committee members of the results. After approval, all items considered by the committee are kept in an Intranet-accessible file for reference.

3.8.6 CLASS CHANGE COMMITTEE

The Department of Leisure Services uses this applications system to administer the classes which they offer and monitor attendance from participants within the citizen community. The change committee reviews change requests, has votes tallied, and is issued results through a coordinator. Approved requests are maintained in an Intranet-accessible file for reference. The application is provided by Active Community Solutions.

KEY I.T. GOVERNANCE FUNCTIONS

3.9 COMMUNICATIONS MANAGEMENT

FEATURED IN THIS SECTION

3.9.1 DEFINITION

3.9.2 OVERVIEW

3.9.3 MODEMS

3.9.4 WIRED COMMUNICATIONS

3.9.5 WIRELESS COMMUNICATIONS

3.9.6 DATA COMMUNICATIONS

COMMUNICATIONS MANAGEMENT

3.9.1 DEFINITION

In this I.T. organization, Communications Management deals with the inventory of telephone, radio, pagers, and similar equipment as well as its installment and maintenance in the workplace together with provision of wired and wireless networking for these devices. Network management for desktop and peripheral computer devices is handled by a separate function within the department. However, the physical wiring used by the computer networking function is provided by this communications management group.

3.9.2 OVERVIEW

At first, it seems that the best way to differentiate this form of communications from the data variety is to label it as "voice." However, many of the voice devices in use today also allow text data and even imaged data to be transported as well. Although not in use at the city as of March, 2005, VOIP (Voice Over Internet Protocol) is a fast-growing technology for transmitting telephone calls over Internet communication routes. Fax machines allow images to be transmitted over phone lines. Further, there is the availability of wireless devices. These multiple avenues have tended to muddle, somewhat, the previous clear distinction between the provision of voice and data communications. Suffice it to say that presently, communications management at the city deals with all forms of communication except for the high-capacity, wired data networkequipment used by computers.

The Communications Engineering and Administration Section of the System Infrastructure Division is the group that:

- Orders new phones and communications devices
- Upgrades existing equipment
- Replaces antennas, batteries, keypads, cases, etc.
- Loans out equipment an a limited basis
- Sends equipment in for repair
- Receives equipment
- Catalogs equipment
- Assigns asset tags to equipment
- Enters equipment information into the I.T. asset management system
- Maintains and loans out audio visual equipment (See Audio/Visual Policy/Procedure)
- Provides data communications cabling and power distribution

COMMUNICATIONS MANAGEMENT

All equipment items valued at more than $5000 (such as servers) are tracked in the Department of Finance and Business Services' Fixed Asset System. (See Fixed Assets Life Cycle for more information.) Lesser-valued items are tracked in the I.T. asset management system maintained by the Communications Engineering and Administration Section of the System Infrastructure Management Division.

All communications equipment and services provided by vendors are contracted with I.T., and then I.T. makes appropriate chargebacks to the various departments on a monthly basis. Policy and procedures for issuance, care, and loss are explained in the Communications Equipment Policy and Communications Equipment Procedure. Approval for issuance of a PDA (Personal Digital Equipment) combination cellular phone/computer device is covered in the Microcomputer Hardware Policy.

3.9.3 MODEMS

One of the principal devices for affecting communications is the modem (modulator-demodulator), which allows computers to transmit information to one another and to data-gathering and display equipment via an ordinary telephone line. There are a number of modem types from different vendors in use as of March, 2005, which serve the diverse applications indicated in the following chart.

Modem Uses

Application	Number	User Group
Ball Field Lighting	30	Traffic Engineering
Dial-up for remote computer access	25	All Departments
Door Access	22	Facilities Management
Duress Alarms	20	Facilities Management
Irrigation	55	Parks and Open Spaces
Sewer Monitoring	22	Public Works
Vehicle Fueling	25	Vehicle Services

COMMUNICATIONS MANAGEMENT

3.9.4 WIRED COMMUNICATIONS

As of March, 2005, there are over 3000 telephones deployed for use by city employees and visiting citizens and vendors. This number is climbing by about 5% per year. Thirty T1 band lines, operating at 1.544 megabits per second with 24 simultaneous channels, give these phones access to the lines of the city's local carrier, Sprint. In contrast to T1 lines, "T3" lines are used for data transmission and have a 44.736 megabit per second capacity, which is sufficient to provide motion video. Also, over 150 fax (facsimile) machines share the T1 lines to provide image transfer capability.

3.9.5 WIRELESS COMMUNICATIONS

In addition to the wired telephones, approximately 600 cellular phones are in use, with both the devices and the service being leased from Verizon and Nextel. Pagers provide one-way communication by delivering a numeric, text, or voice message to a person wirelessly, after which they can respond at their convenience with a different instrument. The city owns approximately 75 pagers of the voice or numeric variety. 67 text pagers and the accompanying service are leased from USA Mobility. The life of the average wireless phone in terms of being up to date and supported by vendors is about one year.

PDAs (Personal Digital Assistants) are combination cell phone, fax, and computer hand-held devices that can provide Internet connection. Over 150 PDAs are in service as of March, 2005, with the demand increasing each year. An especially popular version is the "BlackBerry," which is extremely versatile and is now leased by many service-providing companies. The BlackBerry is a keyboard-equipped, hand-held device manufactured by Research in Motion, Inc.

While discussing wireless communication modes, we cannot neglect what started it all – radios. Two-way devices are commonly used by workers in the field and their bases of operations. The city is licensed by the FCC for 10 frequencies, 4 VHF (Very High Frequency – 30 to 300 Megahertz) and 6 UHF (Ultra High Frequency – 300 to 3000 Megahertz) to serve as carriers for the 550 radios now in use. Of this number, about 80% are owned and serviced by the city, with the other 20% being provided by SNACC (Southern Nevada Area Communications Council), which also provides the carrier frequencies. The city's radios are being converted to SNACC-provided at the rate of about 10% per year, with the goal of eventually having this service completely outsourced. In this arrangement, I.T. still inventories the radios for issuance to departmental users.

COMMUNICATIONS MANAGEMENT

3.9.7 DATA COMMUNICATIONS

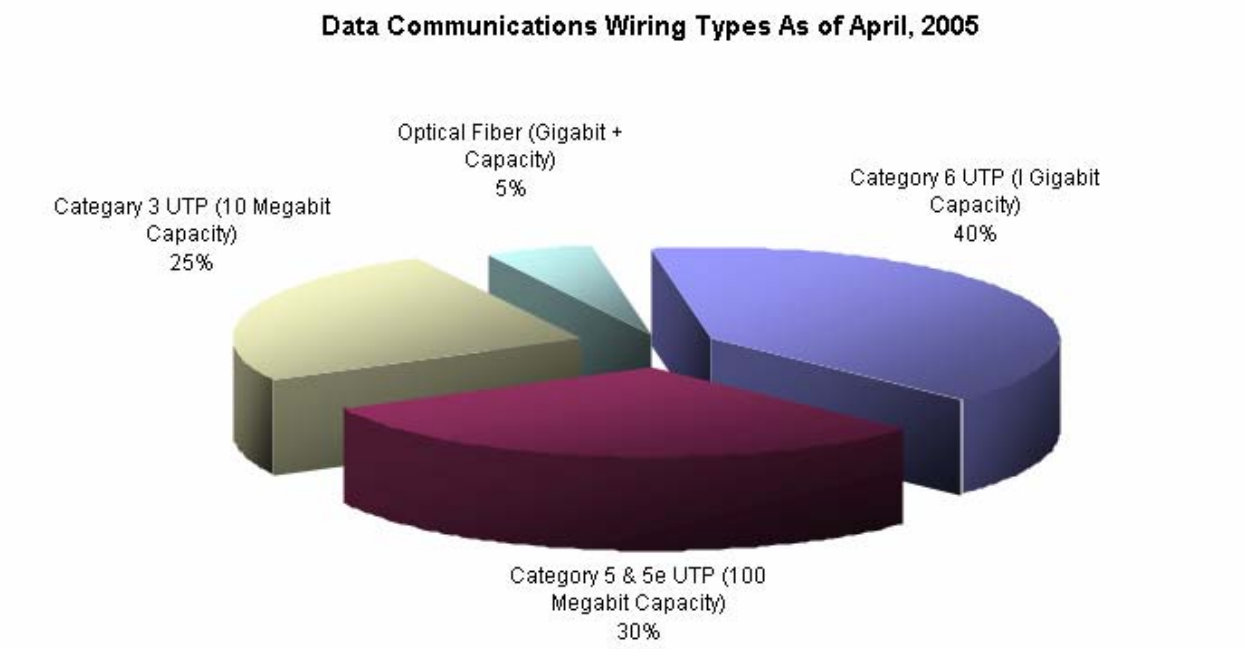
The data communications infrastructure refers to the system of cables and connectors used to facilitate communications between individual pieces of equipment that comprise a computer network, such as PCs, switches, routers, and servers. The city's Data Communications Electrician's primary objectives are to provide state-of-the-art communications infrastructure and power distribution systems. To achieve these objectives, the guidelines below are followed:

- Adhere to industry standards for data communications system planning, design, testing, documentation, implementation, and maintenance. These standards are established by the Telecommunications Industry Association (TIA).
- Stay current with new technologies and standards.
- Adopt new standards when ratified.
- Implement new technologies and standards as needed to accommodate growth and requirements.
- Coordinate inter-departmental data communications requirements.
- Monitor data communications and power systems condition and performance on a continuing basis.

With the introduction of UTP (unshielded twisted pair) cable in the early 1990's, the city adopted this technology as its standard. Next, the termination hardware of several manufacturers was tested in an effort to develop a structured cabling system that would be flexible, reliable, and provide a solid foundation for data communication needs well into the future. Hubbell became the hardware manufacturer of choice, and Commscope was chosen as the cabling solution.

The city data communications infrastructure started with only a dozen or so nodes of Category 3 UTP and has grown to several thousand in the last ten years, with Category 6 UTP now the standard. Multi mode and single mode fiber optic cabling is also being used in the higher speed and higher bandwidth areas of the infrastructure. Category 6e (Category 6 "enhanced") will no doubt see use as soon as it is ratified as a standard by the TIA. A chart showing the different types of cabling now in use follows:

COMMUNICATIONS MANAGEMENT



Keeping a large data communications system running smoothly requires clean, efficient power. The city utilizes Uninterruptible Power Supply (UPS) systems, up to 100 KVA (kilovolt-amp) in capacity, to eliminate power fluctuations commonly observed in commercially-supplied power. When network problems occur, as a matter of routine, the data cable is checked out and eliminated as a suspect first; then the communications equipment at each end is scrutinized. This is because cables are often situated out of sight and can easily be cut by machinery operating too closely.

KEY I.T. GOVERNANCE FUNCTIONS

3.10 COMPUTER OPERATIONS

FEATURED IN THIS SECTION

3.10.1 DEFINITION

3.10.2 OVERVIEW

3.10.3 BACKUPS

COMPUTER OPERATIONS

DEFINITION

I.T. Computer Operations involves ensuring that computer equipment such as servers and mainframes are operational during required hours and that the jobs for which they are scheduled are performed.

3.10.2 OVERVIEW.

Computer Operations embraces three major areas, each of which is associated with a particular 8-hour period of day for which it is best suited:

- Day shift (7:00 am – 3:00 pm) – supporting online operations by ensuring that required equipment is functional
- Swing shift (3:00 pm – 11:00 pm) – running batch jobs and producing large printouts, such as bills for mailing
- Midnight shift (11:00 pm – 7:00 am) – performing system backups

Computer systems technicians' work 10-hour shifts four days per week while the staff provides 24-hour, 7-day-per-week coverage. During overlapping periods, the departing technician passes on system status information to the technician arriving and they assist one another in performing tasks. Work duties include:

- Review and analyze activity logs for security and/or system issues, trends, and problems; prepare and submit reports and analyses to Systems Administration Specialists and management as needed.
- Monitor computer systems and networks for loading and utilization problems and take corrective actions; log and report all anomalies.
- Perform preventive maintenance.
- Ensure use of proper data storage procedures.
- Perform initial systems and network troubleshooting when problems arise; correct minor problems where possible; notify appropriate staff and vendors of needed service or action; assist Systems Administration Specialists in resolving more complex problems.
- Start up and shut down mainframe systems and servers as necessary.
- Schedule jobs and monitor output.
- Run batch jobs and print reports.
- Perform system backups and, when necessary, restore operations; maintain the tape library; coordinate the routing of backup tapes to offsite storage locations. (See additional information on backup procedures below.)
- Assist with the installation of new systems hardware and software.

COMPUTER OPERATIONS

- Provide elementary support desk functions during the hours the support desk is not staffed; coordinate the notification and dispatching of appropriate technical staff; monitor and document the progress of problem resolution.
- Maintain system records, including service and systems failure logs.

Higher-level tasks associated with the computer operations function are to:

- Recommend and assist in the implementation of goals and objectives; implement approved policies and procedures.
- Assist in consulting with other city departments to determine computer system needs; develop plans to integrate I.T. computer systems with other city data processing systems to achieve solutions.
- Work with committees to coordinate the development of standards for both computers and network devices that will ensure functionality between departments and between systems.
- Coordinate with systems administrators regarding the appropriate timing of new software releases, coordinating the installation with I.T. staff and client departments.
- Coordinate and assist with the development of specifications for the city's systems software maintenance contracts.
- Analyze hardware and software products, make appropriate recommendations and coordinate the preparation of specifications; coordinate with vendors to solicit pricing, equipment specifications, and delivery scheduling; discuss new products and maintenance.
- Coordinate computer network administration tasks with systems administration staff.
- Coordinate the development of policies and procedures for computer operations.
- Maintain the inventory of the city's computer room hardware and peripheral equipment.
- Prepare technical reports and make presentations.
- Perform liaison functions between I.T. and other city departments as well as outside agencies whose systems or services interact with city systems.

COMPUTER OPERATIONS

3.10.3 BACKUPS

One of the major responsibilities of the computer operations function is performing backups on a strictly-scheduled basis. These backup files, stored both on and offsite, may be the only way of restoring a database to normal after a system hardware or application software failure. Backups are done nightly for all production databases, and a full system backup is done weekly. For systems requiring 24 x 7 availability, hot backups (while the system is running) are utilized. Systems that are only needed during normal business hours are backed up cold on evenings and weekends and are off-line for about one hour. Logical backups are also taken periodically and stored on separate storage devices and then backed up to tape. Tapes are stored in offsite locations according to a carefully-followed procedure that provides for recycling of tapes after required record storage periods have elapsed.

KEY I.T. GOVERNANCE FUNCTIONS

3.11 COST ALLOCATION

FEATURED IN THIS SECTION

3.11.1 DEFINITION

3.11.2 OVERVIEW

COST ALLOCATION

3.11.1 DEFINITION

Cost allocation refers to a method of assigning indirect, general, and administrative costs for activities, functions, or outputs between entities to ensure that the full cost of delivery is measured. The objective is typically to allocate a known cost among several entities, for example, the cost per unit of resource.

3.11.2 OVERVIEW

Cost allocation is particularly useful when a department is charging other enterprise organizations for services, as with I.T.'s charging other city departments for microcomputer expenses involved with the purchasing and maintenance of hardware and standardized software. This activity, particularly in terms of resources, is also discussed under portfolio management.

The two areas in which I.T. uses cost allocation most directly is (1) providing graphic arts services to departmental clients; and (2) providing desktop PC services including operating, utility, and application software, software upgrades, networking, hardware, and periodic hardware replacement in accordance with organizational security policies and interests. When assigning "indirect" costs to a particular customer's order or to the entire service provided to all departments, this refers to rearranging costs to cross internal I.T. organizational lines so that a reliable number can be obtained to use in calculating chargeback figures.

It is a future goal of I.T. to charge departments for all services rendered, in which case cost allocation covering all project-related expenses would be performed along project lines in addition to the traditional organizational way. As of 2005, the online time card system allows employees' work to be tracked by project.

KEY I.T. GOVERNANCE FUNCTIONS

3.12 DATA MANAGEMENT

FEATURED IN THIS SECTION

3.12.1 DEFINITION

3.12.2 OVERVIEW

3.12.3 DATABASES

3.12.4 BACKUP0/RECOVERY

3.12.5 MONITORING/MAINTENANCE

DATA MANAGEMENT

3.7.1 DEFINITION

Data management involves the planning, development, implementation, and administration of systems for the acquisition, storage, and retrieval of data.

3.7.2 OVERVIEW

The Department of Information Technologies (I.T.) Data Management group's primary objective is to administer and manage the city's information databases.

To achieve this objective, Data Management is responsible for the following:

- Conducting long and short term database planning to support the operational and administrative requirements of the city; advising management on technologies pertinent to data management and Enterprise Resource Program (ERP) implementation; architecting the database implementation of ERP's and coordinating systems software and hardware upgrades from a database perspective
- Developing and enforcing data system standards and procedures; recommending policy governing data and information resource management; determining the city's data information requirements
- Evaluating and monitoring database system performance and performing advanced tuning; recommending and performing system enhancements and upgrades to improve performance, reliability, quality, and integrity
- Designing, implementing, and monitoring data backup and archive plans
- Providing consulting services to functional users and systems development staff and acting as liaison with vendors and other sources of technical support, including other government agencies
- Researching data failures for resolution and to prevent recurrence; investigating and implementing tools for monitoring system performance and health; developing and implementing methods for reporting performance to management
- Participating in the planning and implementation of ERP and other software projects; providing recommendations and guidance on database instance strategy, configuration, and change control.

DATA MANAGEMENT

3.7.2 DATABASES

The majority of the information for all enterprise business and ERP applications are hosted in Oracle Databases, with some workgroup level applications using Microsoft SQL Server.

The following table lists the current configured production databases and major application groups:

Current CLV Databases				March 2005
Version	**Size**	**Concurrent Users (Avg)**	**Applications**	**User Group**
Oracle 8.1.7 (upgrade to 9.2.05 planned)	90GB	350	Oracle Applications 11i	Finance, Human Resources (HR)
Oracle 7.3.4 (planned for retire-ment)	10GB	10	Pyramid	Insurance Services In HR
Oracle 8.1.7 (upgrade to 9.2.05 planned)	130GB	120	ESRI GIS SDE (Environmental Research Systems Institute - Geographic Info Systems) External Web Applications	GIS users Citizens
Oracle 8.1.7 (upgrade to 9.2.05 planned)	40GB	400	Hansen 7.x Class 4.x Pcard Courts Alternative Sentencing In-house Developed Systems	Business Services, Public Works, Building and Safety Leisure Services Purchasing In Finance Municipal Courts Various departments

(Continued)

DATA MANAGEMENT

Version	Size	Concurrent Users (Avg)	Applications	User Group
Oracle 8.1.7 (upgrade to 9.2.05 planned)	35GB	2	Factory Link (SCADA)	WPCF (Wastewater Pollution Control Facility) – Main
	10GB	2		WPCF – Durango Facility
	5GB	2		WPCF – BOMO Site
SQL Server 2000	20GB	80	HEAT (Help Expert Automation Tool)	All users
			Cardinal	Parking Enforcement
			Emeritus	Fire Employee Health
			eAgenda	City Clerk, City Council
			ProLaw 9.x	City Attorney
			MyNevada (Web site)	Citizens
			Other In-house-Developed Systems	Various departments
SyBase		625	TeleStaff 1.x	Fire personnel
Unisys (Legacy)	13GB	122	Courts	Municipal Courts
	2	26	Jail	Detention and Enforcement
	4	69	Build	Building and Safety
	0.2	3	Garage	Vehicle Services
	2	35	Business	Business Services

3.7.3 BACKUP/RECOVERY

To ensure that availability requirements are met, all Oracle database configurations are based on the OFA (Oracle Flexible Architecture) guidelines. They provide recommendations for the layout of control files, system data files, redo logs, archive logs, application data files, temporary tablespaces, and rollback segments. All systems use RAID (Redundant Arrayed Independent Disk) storage to reduce the risk of disk failures, and spare drives are kept in-house.

DATA MANAGEMENT

Backups are done nightly for all production databases, and a full system backup is done weekly. For systems requiring 24 x 7 availability, hot backups are utilized. Systems that are only needed during normal business hours are backed up cold and are off-line for about 1 hour. Logical backups (extractions from a database to a flat file) are also taken periodically and stored on separate storage devices and then backed up to tape.

3.7.4 MONITORING/MAINTENANCE

Database monitoring and maintenance are done on a regular schedule and are organized by daily, weekly and monthly processes. Daily processes focus on ensuring that:

- Everything, including databases, network, and alert monitoring agents are available and performing normally
- The scheduled backups were successful.

Weekly processes focus on tablespace and database object maintenance as well as database integrity checking. Monthly processes are aimed at reviewing the previous month's statistics and comparing them to history to look for:

- Harmful growth rates
- Opportunities to improve performance

KEY I.T. GOVERNANCE FUNCTIONS

3.13 DESKTOP SUPPORT

FEATURED IN THIS SECTION

3.13.1 DEFINITION

3.13.2 OVERVIEW

3.13.3 RESPONSIBILITIES

3.13.4 SOLUTIONS

DESKTOP SUPPORT

3.13.1 DEFINITION

Desktop Support involves the procurement, installation, configuration, and support, of all desktop hardware, software, and peripherals as well as maintaining the inventory of these items. This function is performed by the Client Support Section of the Applications Services Division of the Department of Information Technologies (I.T.).

3.13.2 OVERVIEW

To carry out their objectives, Client Support is responsible for the following:

- Research microcomputer systems to determine specifications for City of Las Vegas standards each year.
- Prepare a standard image for City of Las Vegas microcomputer software annually.
  - Conduct testing of these new systems.
  - Present findings to I.T. Configuration Control Committee (ITCCC) for review and approval.
- Maintain all city desktop hardware and peripheral devices (e.g., printers, PDAs, etc.).
- Maintain all city desktop software.
- Research and maintain all desktop security patches and necessary updates for all city software.
  - Conduct testing of these new systems
  - Present findings to ITCCC for review and approval.
- Purchase all IT-related hardware, software, and peripherals.
  - Track all of these items through their life cycle
  - Prepare all retired equipment and surplus items according to NRS (Nevada Revised Statutes) rules.
- Provide hands-on training for computer software, hardware (such as BlackBerry devices) and system use; oversee the preparation of documentation for training or instruction.
- Appraise, recommend, and implement enterprise computer solutions.
- Serve as primary consultant to city departments to determine microcomputer needs; provide advanced technical assistance for microcomputer systems and programs.
- Provide Audio/Visual support.
  - For City of Las Vegas departments.
  - For all Council-sponsored neighborhood events.

DESKTOP SUPPORT

- Provide first-level customer support for all city employees' IT-related issues.
  - Enter requests into department call-logging system and assign to responsible parties.
  - Monitor calls to ensure compliance with SLAs (Service Level Agreements).
  - Review calls to ensure information accuracy for chargebacks.
  - Compile statistical reports to show performance and trends.

3.13.2 RESPONSIBILITIES

Client Support currently (as of April, 2005) is responsible for, and provides support for, more than 2200 desktop computers; most of which are supplied by Dell Corporation. Support is also provided for over 1400 printers; which are mostly Hewlett Packard models, and over 225 PDA devices; which are mostly Blackberry wireless devices.

There are currently (as of April, 2005) over 1400 different software applications in use at the city, with their users spread among over 100 locations (not all of them networked) throughout the city boundaries. A document, Reporting Microcomputer Problems, is provided on the Intranet to explain the reporting process for clients.

3.13.4 SOLUTIONS

The IT Support Desk receives an average of 104 calls per day. Not all of these are calls requiring problem resolution. Of those that are, Client Support resolves over 60%. The remaining calls are assigned to other divisions of IT or to other departments as appropriate. An example of where this commonly occurs would be client requests for hardware peripherals and software, which Client Support reviews for adherence to standards and then passes to the Purchasing Division of the Department of Finance and Business Services if compliant.

The client support team has developed an advantageous inventory approach whereby the entire incident inventory is stored within the HEAT (Help Expert Automation Tool) call logging system. This has eliminated the previous need to store information in several different databases as well as reduced the number of typographical errors resulting from multiple entries.

Client support has also helped to develop an interface that calculates the monthly charges for services provided and exports them directly into the Oracle G/L (General Ledger) system. This eliminated the old, more cumbersome process, which was to put all of the client support transactions onto Excel spreadsheets and have Finance do manual month-end postings into the G/L.

DESKTOP SUPPORT

The client support group is well organized and functions effectively as a team. Each morning a short staff meeting is held to keep everyone up on the previous workday's significant events and to prepare them for the day ahead. All of client support's installation instructions and frequently-asked questions are posted on a central website for easy access. (A sample I.T. Client Support home page is provided in the Appendix.) Whenever a new problem is encountered, it is written up and posted on the web site so that in the future other team members won't have to duplicate the required research. If the problem is not one listed on the local site, the now-familiar-tio-everyone Google Internet site imay be scrutinized. Of course, supplier web sites are also available. Each time a new application is introduced at the city, client support is required to test and document it for review and approval by ITCCC voting members. During this process client support also writes up installation instructions that are posted on this site so that anyone within the group could install that particular software in the future.

The "support ratio" is the number of desktop units (including laptops – but not blackberries and other PDA devices) divided by the number of desktop support persons. According to Gartner, the national average for the support ratio is 75 to 1. So does our 220 to 1 (2200 desktops and 10 microcomputer specialists) mean we are stretched too thin and not providing sufficient support or support quality? We don't think so, due to the emphasis we have placed on documentation of prior calls and on standardization of desktop hardware and software products, which keeps our call volume lower to begin with. Often help desk calls are prevented simply by the fact that the person in the client work area sitting nearby uses the same product and can provide a ready answer. One of the reasons we appreciate standardization at the desktop level is that we don't have it with departmental applications, since so many are vendor-provided and frequently require involved hardware and software interfacing.

KEY I.T. GOVERNANCE FUNCTIONS

3.14 eGOVERNMENT PLANNING AND ADMINISTRATION

FEATURED IN THIS SECTION

3.14.1 DEFINITION

3.14.2 OVERVIEW

3.14.3 SPECIFIC FUNCTIONS

eGOVERNMENT PLANNING AND ADMININSTRATION

3.14.1 DEFINITION

Delivering government services and exchanging information with citizens, businesses and other agencies on a 24 hour, 7-day-per-week basis through web-based portals.

3.14.2 OVERVIEW

The Internet has revolutionized the way people work, learn, play and use business and government services. The public is becoming more accustomed to the ease, convenience and flexibility of using technology in their personal and professional lives. It is becoming routine to check account balances, transfer funds and pay bills at bank web sites, for example, or to purchase goods and services online. The entire process of purchasing travel can now be done electronically – from researching destinations, to making car or hotel reservations, to buying tickets. Today it is even possible to check in for a commercial flight on a home computer or using a touch screen kiosk at the airport.

As the business community embraces the tremendous opportunities to provide even better service to customers over the Internet, expectations are rapidly expanding regarding what consumers should be able to do online. A self-service culture is developing where people demand access to information and services day or night at *their* convenience. Municipalities must match the higher levels of electronic service required by more technologically sophisticated citizens.

The City of Las Vegas Department of Information Technologies (I.T.) is committed to remaining innovative and forward-thinking in order to stay ahead of these expectations. In that spirit we have written this document formalizing our vision and strategic plan for bringing effective electronic government to constituents.

As of 2005, most eGovernment services offered by the city are delivered through the web site at www.lasvegasnevada.gov. Responsibility for the site's maintenance is shared by I.T., the Office of Communications, and departmental contributors.

eGOVERNMENT PLANNING AND ADMININSTRATION

3.14.3 SPECIFIC FUNCTIONS

The specific functions are as follows:

Department of Information Technologies	Office of Communications	Department Content Contributor
Owns the infrastructure	**Owns the web content**	**Owns the business process**
• decides on the technology, navigation, look-and-feel of the site • maintains the RedDot content management system used by content contributors to update the site • recommends and develops web applications for city departments • provides project management expertise in the development of new services • educates the organization about technology solutions	• ensures all web communications properly reflect the city's "brand" • develops standards for writing style and consistency on the site • approves content changes before they can go live	• writes and edits the content for an individual department's web pages • submits web page updates through the RedDot content management system for approval by the Office of Communications

Every effort is being made to engineer the website to provide a customer-oriented "look and feel." This means less emphasis on displaying web services via traditional departmental lines, where this can be a handicap to citizens trying to locate a service quickly. An example of the current Internet home page is provided in the Appendix.

eGOVERNMENT PLANNING AND ADMININSTRATION

Current services

Current eGovernment services offered include:

- Pay parking tickets online
- Online sewer payments
- Online traffic school
- Interactive business licensing (apply, search)
- Permit status
- eAgenda (City Council meeting agendas)
- Register for Leisure Services classes
- Citizen complaints
- On demand video (watch KCLV-TV, Council meetings, public service announcements, etc.)
- Interactive maps
- Online customer support using live chat
- Online traffic cams at major intersections

Future services

Planned eGovernment services include:

- Online job application
- Better support for other languages
- Shared (with other government agencies) services
- Intranet (employees' web site) redesign
- Increase and promote use of automated phone services
- Develop and display walk-through permits and business licenses
- Provide for citizen self-service with online signups at counter sites or kiosks
- Establish tracking and reports of all citizen feedback
- Garage/yard sale registrations
- Online scheduling of building inspections
- Online subcontractor registration

KEY I.T. GOVERNANCE FUNCTIONS

3.15 NETWORK MANAGEMENT

FEATURED IN THIS SECTION

3.15.1 DEFINITION

3.15.2 OVERVIEW

3.15.3 NETWORK CONNECTIONS

3.15.4 DESIGN AND REDUNDANCY

3.15.5 MONITORING

NETWORK MANAGEMENT

3.15.1 DEFINITION

Network management includes the processes of managing, monitoring, and controlling a communications network. Modern Network Management systems also include the ability to re-configure network elements remotely.

A wide variety of software and hardware products are available to help network system administrators manage a network. Network management covers these important functions:
Security - Ensuring that the network is protected from unauthorized users
Performance - Eliminating bottlenecks in the network
Reliability - Making sure the network is available to users and responding to hardware and software malfunctions.

3.15.2 OVERVIEW

The Department of Information Technologies (I.T.) Network Engineering group's primary objective is to administer and manage the city's information networks and to administer and support the city's Internet and Intranet. Voice communications, cabling, and networking (for administration, inventory, etc.) are discussed in Communications Management.

To achieve this objective, the responsible Systems Administration Specialists perform the following:

- Conducting long and short term network planning to support the operational and administrative requirements of the city; advising management on technologies pertinent to network management and implementation; and coordinating systems communications upgrades from a network perspective
- Developing and enforcing network system standards and procedures; recommending policy governing network management; determining the city's networking requirements
- Proactive evaluation of network performance; recommending and installing enhancements and upgrades to improve performance and reliability
- Research and work with service providers to ensure the most cost-effective and reliable solution for Wide Area Network connections are provided to city users
- Providing consulting services to functional users and systems development staff and acting as liaison with vendors and other sources of technical support, including other government agencies
- Researching network failures for resolution and to prevent recurrence; investigating and implementing tools for monitoring network performance and health; developing and implementing methods for reporting performance to management

NETWORK MANAGEMENT

- Securing the connections between the city network, Internet, wireless provider networks, remote workforce and work from home, and connected agencies. Providing secure 802.11 wireless networks
- Interpreting and developing compliance strategies for Federal security standards
- Configuring and maintaining firewall, NBAD (Network Behavior Anomaly Detection), proxy server, host ips, and other network security technologies
- Maintaining archive of security and network equipment log files
- Monitoring security threats that are constantly emerging, and advising management on security strategies and best practices
- Developing network equipment security policies

3.15.3 NETWORK CONNECTIONS

We could list all of the network connections to the over 50 locations served by the city's network, but it is probably more appropriate to simply state that as of February, 2005 there are over 90 connections, or nodes in the network.

3.15.4 DESIGN AND REDUNDANCY

To ensure that networks are properly designed from a reliability and security perspective, Cisco Corporation's SAFE network architecture and Cisco-switched and routed network design guides are adhered to.

3.15.5 MONITORING

The network is monitored 24 x 7 by I.T. staff using different network monitoring packages. Automatic notifications and escalation procedures are in place and used in the event of a problem.

KEY I.T. GOVERNANCE FUNCTIONS

3.16 PORTFOLIO MANAGEMENT

FEATURED IN THIS SECTION

3.16.1 DEFINITION

3.16.2 OVERVIEW

3.16.3 NEXT STEPS

PORTFOLIO MANAGEMENT

3.16.1 DEFINITION

Information Technologies Portfolio Management involves the provision of resources by the Department of Information Technologies (I.T.) to departmental customers through a predefined set of broad-based services that encompass all new and ongoing projects. In some cases, I.T. receives reimbursement from departments for particular types of service, based upon selected criteria.

3.16.2 OVERVIEW

Having resources aligned and committed according to new and existing projects instead of only by traditional organizational lines allows those resources to more readily be aligned with strategic objectives. It also provides a more reliable way to arrive at project costs. In order to do this accurately, an automated tool needs to be utilized. As of 2005, I.T. is in the process of adapting resource allocation to Microsoft's Project 2003 management software. Additionally, the Process On Demand system for defining and linking project templates, from BOT International, is being implemented to document necessary steps in the process flow and thus provide increased accountability.

An example of portfolio management involving departmental reimbursement would be the provision of desktop PC services including operating, utility, and application software, software upgrades, networking, hardware, and periodic hardware replacement in accordance with organizational security policies and interests. The annual amount charged back to departments through an Internal Service Fund (ISD) for this group of services is arrived at based on I.T.'s costs involved with service delivery and the number of units supported. Desktop units delivered in mid-year have the charges prorated.

Another support function within I.T. that is managed in this way is Graphic Arts. This group produces specialized printing for departmental customers, often in large volume, for flyers, special announcements, etc., as well as posters both large and small. Departments requiring production of this kind of material contract with Graphic Arts to have it produced and then transfer funds to I.T. upon successful project completion through an ISF.

PORTFOLIO MANAGEMENT

3.16.3 NEXT STEPS

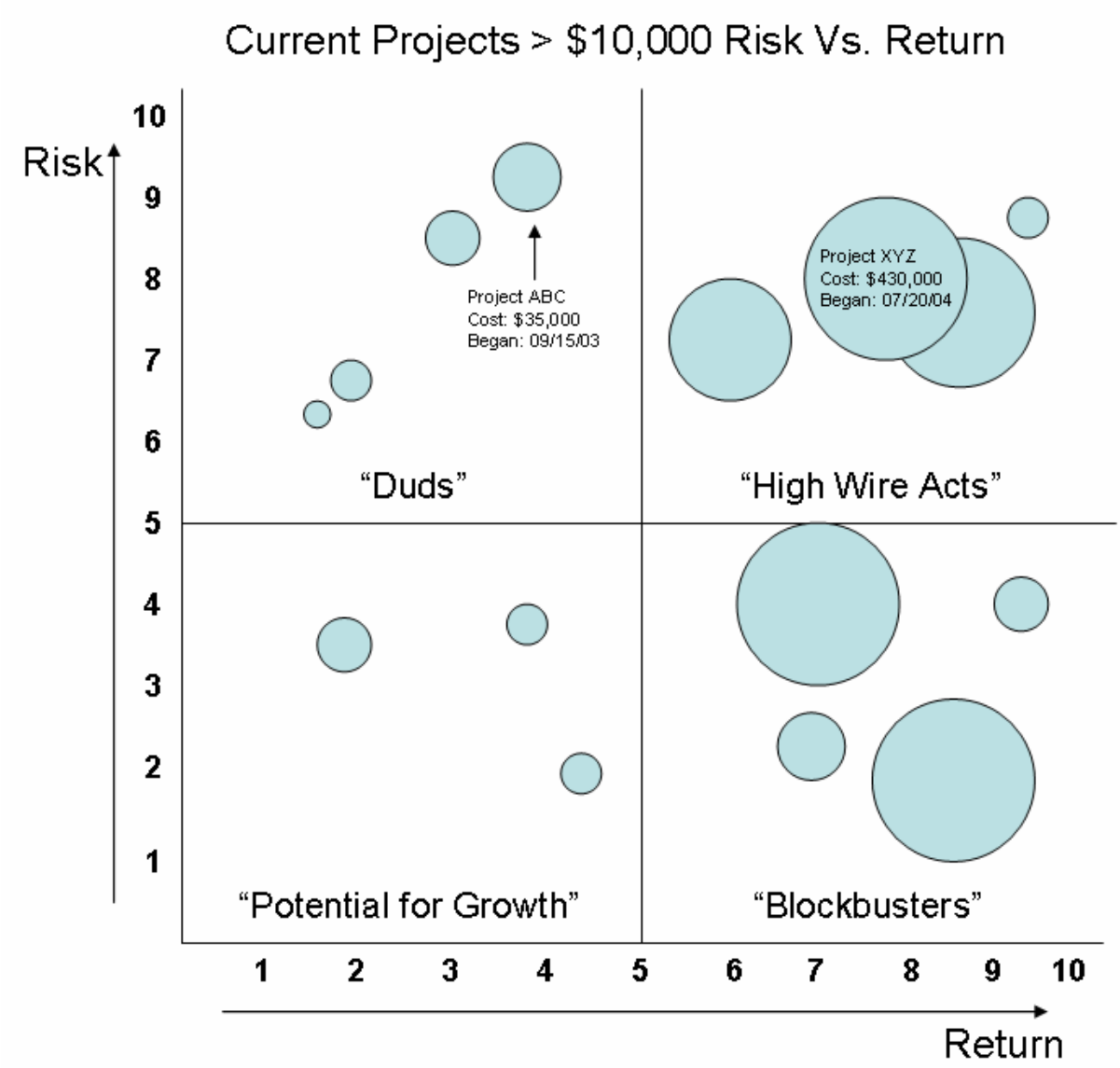
It is the eventual goal of I.T. to have all of its services charged back to departmental customers, in particular, application software development. Applications would have amounts budgeted based upon estimated number of project hours and then have the amounts charged to the departmental customers through an ISF based on the actual number of project hours necessary. The amount per hour would be fixed according to I.T.'s recovery of costs. A Services Catalog describing the services that I.T. offers is being prepared.

I.T. is looking at how other governmental entities have implemented this change and the budgeting and operations modifications that would be required to support it. A big advantage for portfolio management in the delivery of applications is that it helps control "feature creep." This occurs when agreements are made, systems are designed and constructed, but delivery dates are missed because users want improvements to the system continually during development, thus invalidating original delivery date estimates. In a portfolio-managed operation, contracts for specific systems are agreed upon by the parties involved, and feature changes are contracted in later versions.

Ideally, a portfolio management system involves a scorecard process for ranking projects in terms of opposing categories, such as risk vs. return. Then key management staff periodically decide which projects to cancel, to continue to support, or to increase resources for, based upon how they rank in a graph reflecting winners and losers, as well as projects with a potential for growth or for continued maintenance. A sample graph depicting quadrant placement might appear as below:

PORTFOLIO MANAGEMENT

Sample Chart of Projects Showing Risk vs. Return



KEY I.T. GOVERNANCE FUNCTIONS

3.17 PROJECT MANAGEMENT

FEATURED IN THIS SECTION

3.17.1 DEFINITION

3.17.2 OVERVIEW

3.17.3 THE MODEL

3.17.4 PROJECT MANAGEMENT KNOWLEDGE AREAS

3.17.5 CLV STANDARD PROJECT PROCESS STEPS

PROJECT MANAGEMENT

3.17.1 DEFINITION

Project Management within the Department of Information Technologies (I.T.) is the application of knowledge, skills, tools and techniques to a broad range of activities to meet the requirements of the particular project.

3.17.2 OVERVIEW

Project management knowledge and practices are best described in terms of seven component processes.

1. Selection (Is the work to be done a project or merely a task?)
2. Initiating
3. Planning
4. Executing
5. Controlling
6. Closing (Implementation)
7. Continuous Improvement (Maintenance)

The processes can also be divided into nine project knowledge management areas:

1. Integration
2. Scope
3. Time
4. Cost
5. Quality
6. Human resources
7. Communications
8. Risk
9. Procurement

The seven processes can be expanded into twelve CLV standard project process steps that have gates added at the appropriate places to reflect work that must be completed before proceeding to the next step. Numbering steps in this way keeps the overall numbering scheme of the processes intact. The individual work items to be completed within a process can then be assigned unique numbers within the following categories.

PROJECT MANAGEMENT

1.0 Project Selection
1.99 Project Selection Gate
2.0 Initiating
2.99 Initiating Gate
3.0 Planning
3.99 Planning Gate
4.0 Executing
5.0 Controlling
5.99 Controlling Gate
6.0 Closing
6.99 Closing Gate
7.0 Continuous Improvement

3.17.3 THE MODEL

Project management experts and books abound. The problem in pursuing best practices is that every author and method has a different approach, differing areas of concentration, and particularly, different terminology. The Project Management Institute (PMI) has already performed considerable reconciliation research and created one repository for best practices as they relate to project management. This information is contained in PMI's "A Guide to the Project Management Body of Knowledge (PMBOK)". PMI states that PMBOK "is an inclusive term that describes the sum of knowledge within the profession of project management." PMI further certifies that the PMBOK Guide is "generally accepted," meaning that "the knowledge and practices described are applicable to most projects most of the time, and that there is widespread consensus about their value and usefulness."

An example of the conciseness yet thoroughness embodied in PMBOK instruction is demonstrated by how PMI defines project process in the PMBOK guide:
Projects are composed of processes. A process is "a series of actions bringing about a result." Project processes are performed by people and generally fall into one of two major categories:

- *Project management processes describe, organize, and complete the work of the project. The project management processes that are applicable to most projects, most of the time, are described in more detail below.*
- *Product-oriented processes specify and create the project's product. Product-oriented processes are typically defined by the project life cycle and vary by application area.*

Project management processes and product-oriented processes overlap and interact throughout the project. For example, the scope of the project cannot be defined in the absence of some basic understanding of how to create the product.

PROJECT MANAGEMENT

I.T.-related projects at the city fall into two broad groups:

- **Enterprise projects** cross departmental lines, have high citizen or customer visibility, are sensitive or confidential in nature, are requested by the City Manager's office or elected officials, or are funded by the Information Technologies capital projects budget. These projects are managed by Enterprise Project Managers.
- **I.T. projects** are managed by I.T. Project Coordinators and include all other technology projects.

The I.T. Client Relationship Services Division is charged with project management, with the actual project management being carried out by project coordinators. All of the project coordinators working within this division either have received, or are in the process of acquiring, certification from PMI. The I.T. Client Relationship Services Division, as of February 2005, uses an inhouse-developed Project Charter document for tracking the component processes involved in project development. This document is in agreement with project processes as defined by PMI. The template is available in the Appendix.

3.17.4 PROJECT MANAGEMENT KNOWLEDGE AREAS

The nine project knowledge areas are described below in more detail Subsets describe PMI best practice processes within each knowledge area group. I.T. Client Relationship Services endorses this concept and utilizes these knowledge areas in a tailored approach for each individual project.

Project Integration *– ensuring that the various elements of the project are properly coordinated.*

- Project plan development – integrate and coordinate all project plan elements to create consistent, coherent plan documents.
- Project plan execution – carry out the project plan by performing all activities specified within plan documents.
- Integrated change control – coordinate changes across the entire project. Reflect changes during the development phase in the project charter. Changes involving implementation into a live environment are voted upon by committees designated for specific application areas. The current functioning change control groups are:
  - I.T. Configuration Control Committee (enterprise-wide changes)
  - Oracle Change Review Committee
  - Hansen Change Committee
  - Class Change Committee

PROJECT MANAGEMENT

Project Scope *– ensure that the project includes all the work required, and only the work required, to complete the project successfully.*

- Initiation – authorize the project or phase.
- Scope planning – develop a written scope statement as the basis for future project decisions. This scope statement is part of the Project Charter.
- Scope definition – subdivide the major project deliverables into smaller, more manageable components.
- Scope verification – formalize acceptance of the project scope.
- Scope change control – document all changes to project scope by updating scope section of Project Charter.

Project Time *– ensure timely completion of the project.*

- Activity definition – identify specific activities that must be performed to produce the various project deliverables.
- Activity sequencing – identify and document dependencies between activities.
- Activity duration estimating – estimate the number of man-days that will be needed to complete individual activities. Experience is increasing reliability here.
- Schedule development – analyze activity sequences, activity durations, and resource requirements to create the project schedule.
- Schedule control – control changes to the project schedule.

Project Cost *– ensure that the project is completed within the approved budget.*

- Resource planning – determine what resources (people, equipment, materials) and what quantities of each should be used to perform project activities.
- Cost estimating – develop an approximation (estimate) of the costs of the resources needed to complete project activities.
- Cost budgeting – allocate the overall cost estimate to individual work activities.
- Cost control – control changes to the project budget.
- ROI (Return On Investment) – Attempt to assess the value of the project, either through direct cost justification or indirectly.

Project Quality *– ensure that the project will satisfy the needs for which it was undertaken.*

- Quality planning – identify which quality standards are relevant to the project, and determine how to satisfy them.
- Quality assurance – evaluate overall project performance on a regular basis to provide confidence that the project will satisfy the relevant quality standards.
- Quality control – monitor specific project results to determine if they comply with relevant quality standards and identify ways to eliminate causes of unsatisfactory performance. Utilize peer reviews for catching developed software errors early in the process.

PROJECT MANAGEMENT

Project Human Resource *– make the most effective use of the people involved with the project.*

- Organizational planning – identify, document, and assign project roles, responsibilities, and reporting relationships.
- Staff acquisition – get the needed human resources assigned to and working on the project.
- Team development – develop individual and group skills to enhance project performance.

Project Communications *– ensure timely and appropriate generation, collection, dissemination, storage, and ultimate disposition of project information.*

- Communications planning – determine the information and communications needs of the stakeholders: who needs what information, when they will need it, and how it will be given to them.
- Information distribution – make needed information available to project stakeholders in a timely manner.
- Performance reporting – collect and disseminate performance information. This includes status reporting, progress measurement, and forecasting.
- Administrative closure – generate, gather, and disseminate information to formalize phase or project completion.

.

Project Risk *– identify, analyze, and respond to project risk. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events to project objectives.*

- Risk management planning – decide how to approach and plan the risk management activities for a project.
- Risk identification – determine which risks might affect the project and documenting their characteristics.
- Qualitative risk analysis – perform a qualitative analysis of risks and conditions to prioritize their effects on project objectives.
- Risk response planning – develop procedures and techniques to enhance opportunities and reduce threats from risk to the project's objectives. As risks are identified, state mitigation procedures to follow whenever possible. Mitigation procedures are usually stated whenever risks are identified.
- Risk monitoring and control – monitor residual risks, identify new risks, execute risk reduction plans, and evaluate their effectiveness throughout the project life cycle.

PROJECT MANAGEMENT

Project Procurement *– acquire goods and services to attain project scope from outside the performing organization.*

- Procurement planning – determine what to procure and when.
- Solicitation planning – document product requirements and identify potential sources.
- Solicitation – obtain quotations, bids, offers, or proposals, as appropriate.
- Source selection – choose from among potential sellers.
- Contract administration – manage the relationship with the seller.
- Contract closeout – perform completion and settlement of the contract, including resolution of any open items.

3.17.5 CLV STANDARD PROJECT PROCESS STEPS

The CLV standard project process steps for I.T. and the finished work components of each step are outlined in a table in the Appendix. Custom templates have been created for each of the completed work components, so that during the course of a project time is not spent unnecessarily designing templates and so that there is standardization in the work approach from project to project. The work components chosen can vary depending upon the project size. For large and complex projects, a second set of custom templates (numbering over 50), is also available for use.

KEY I.T. GOVERNANCE FUNCTIONS

3.18 QUALITY ASSURANCE

FEATURED IN THIS SECTION

3.18.1 DEFINITION

3.18.2 OVERVIEW

QUALITY ASSURANCE

3.18.1 DEFINITION

Quality Assurance (QA) is a planned and systematic pattern of actions necessary to provide adequate confidence that the product optimally fulfills customers' expectations, i.e., that it is problem-free and well able to perform the task for which it was designed.

3.18.2 OVERVIEW

QA within the Department of Information Technologies (I.T.) is charged with ensuring that all of the necessary components of a change have been accounted for and are performed at an acceptable level. These components include:

- Checking for completion of all steps in the process
- Ensuring that testing has been performed
- Making certain that adequate documentation has been provided
- Ensuring that the change process includes sign-offs by responsible parties at appropriate points
- Making certain that changes are not introduced into the live environment without having followed established change control procedures

The QA function within I.T. is guided by a Quality Assurance Administrator and a Quality Assurance Coordinator. The QA Administrator is tasked 'To develop, implement, coordinate, evaluate, and manage programs designed to ensure the quality of operations of the assigned department or major division and to perform a variety of tasks relative to the area of responsibility.' The QA Administrator within I.T. functions as coordinator for the enterprise's four change committees, develops and reviews policy and procedure documents, performs QA audits, and assists with testing as needed. The QA Administrator also chairs the I.T. Configuration Change Committee and handles its administration.

The QA Coordinator's job is 'To develop, implement, coordinate, evaluate, and manage software testing and training to ensure quality.' Other duties include:

- Work with I.T. functional groups and city business units to perform testing on its hardware and software and communicate the results back to both the change control committees and/or responsible parties.
- Develop and maintain training curricula and associated materials.
- Ensure training and documentation is kept up to date and/or complete through the Project Coordinators or Client Support.
- Coordinate scheduling of training sessions in conjunction with testing and implementation of software, maintain training records, and prepare computer help tools.

QUALITY ASSURANCE

QA seeks to obtain sign-offs and/or formal e-mail voting when having project charters and change requests reviewed by responsible parties as a way of establishing accountability, which, in turn, enhances the prospects for better quality. The QA administrator is not as close to a particular project as the Project Manager or the QA Coordinator (charged with guiding and monitoring testing) and functions much as an auditor would.

KEY I.T. GOVERNANCE FUNCTIONS

3.19 REFERENCE

FEATURED IN THIS SECTION

3.19.1 DEFINITION

3.19.2 OVERVIEW

REFERENCE

3.19.1 DEFINITION

In I.T., reference refers to all documentation describing:

- The planning, organization, and operation of I.T.
- The operation of hardware, applications and operating systems software, databases, network systems, and other computer-related hardware and software
- The maintenance and availability of trouble-shooting information, now commonly provided via easily-accessible web sites

3.19.2 OVERVIEW

In essence, any document describing the operation of I.T. or I.T.-related products is an item of reference. This document is a reference, as are policies and procedures. Because of the service nature of I.T., these documents must be able to be located quickly by staff when needed. This means procedures must be in place to properly store and retrieve the materials.

Generally, reference manuals are provided with all hardware and software products. Years ago, these were always printed and limited to one per device or software licensee. These manuals can be voluminous as well as precious when needed and misplaced. Today, materials are made available both printed and on-line via the web. The on-line versions protect owners from misplacement and allow for printing of only the pages of interest.

Today, approved policies and procedures for all city departments are posted on their individual Intranet web sites. CDs documenting miscellaneous software tools and programming self-teaching are stored in a database maintained by the I.T. Quality Assurance Administrator and records are kept of who checks out or returns what and when. Documentation for desktop software is maintained on-line by the Microcomputer Support Supervisor and accessible via web site. Technical documentation used for maintaining systems and network equipment is obtained from web site sources provided by vendors for use by systems infrastructure staff.

KEY I.T. GOVERNANCE FUNCTIONS

3.20 RESOURCE MANAGEMENT

FEATURED IN THIS SECTION

3.20.1 DEFINITION

3.20.2 OVERVIEW

RESOURCE MANAGEMENT

3.20.1 DEFINITION

Resource management within the Department of Information Technologies (I.T.) includes those actions taken to identify sources and obtain resources needed to support activities; coordinate the allocation of resources among activities so that they are optimally delivered where and when most needed; and maintain accountability for resources and resource use.

3.20.2 OVERVIEW

From a broad point of view, organizational resources can be grouped into three general categories: facilities; machinery, equipment, and software; and human resources. I.T. facilities consist of what has been built or established to allow I.T. to serve the enterprise. I.T. consumes the main City of Las Vegas building's entire fifth floor (housing the computer room as well as office space for management, systems, and applications staff), portions of the basement area (for microcomputer support and the Graphic Arts staff and equipment). Many I.T. organizations today have a remote facility located at least 10 miles away to provide an operational site for critical I.T. functions in the event of a disaster affecting the main facility. As of 2005, I.T. utilizes a dedicated building for the purpose of disaster recovery at the city's West Yard Service Center, situated 10.1 miles distant from the main campus. (See the second page of the Security and Contingency Planning section.)

In terms of equipment, I.T. manages over 100 servers linked with more than 2200 microcomputers over a network connecting more than 50 citywide locations. In order to control problems with equipment incompatibilities, I.T. purchases all servers, microcomputers, and networking equipment used by city departments, and carefully tests all new models with existing hardware and software before introduction into the production environment. Software versioning is carefully maintained to also control incompatibilities and to ensure that vendor licensing agreements are honored. All employees are charged with taking proper care of the I.T. resources issued to them and for using those resources responsibly. The associated details are presented to new employees in the form of an Information Resources Use Agreement, which they are required to sign, and a companion Information Resources Use Policy, by which all employees are to abide.

An e-mail system is provided to the enterprise by I.T. to maximize employee communication and to help document decisions. An E-Mail Policy spells out how the system is to be used, and an E-Mail Records Policy describes how to distinguish between documents as records or temporary communications.

RESOURCE MANAGEMENT

Access to the Internet is provided for those employees who need to draw from its vast information content in more efficiently performing their jobs. Information for Las Vegas citizens and visitors is provided on the city's web site at www.lasvegasnevada.gov. The Office of Communications is responsible for managing Internet web content and co-authored the Internet Web Site Content Management Policy with I.T. to explain to employees the guidelines for content preparation and the approvals necessary prior to publication. The use of the Internet by employees is delineated in the Internet Policy and Internet Procedure documents.

Another valuable service provided by I.T. is the Intranet, which allows each of the departments to impart information to employees and eliminates the need for phone calls and personal assistance much of the time. Use of the Intranet is described in the Intranet Policy and companion Intranet Procedure documents. Intranet content is specifically addressed in the Intranet Web Site Content Management Policy. Examples of Intranet services provided for employees are:

- Employee Bulletin Board
- Employee Phone Book
- Policies and Procedures
- Questions for the City Manager
- Questions for the Insurance Manager
- Frequently-Asked-Questions for the I.T. Support Desk
- Job Descriptions
- Job Listings
- Events
- Safety Information
- Weather Reports

As of February, 2005, I.T. is implementing Microsoft's Project 2003 to assist with tracking staff resources according to assigned projects. In addition, a template management system from BOT International is being installed to track project documentation and to assist in maintaining staff accountability for project assignments.

KEY I.T. GOVERNANCE FUNCTIONS

3.21 SECURITY AND CONTINGENCY PLANNING

FEATURED IN THIS SECTION

3.21.1 DEFINITION

3.21.2 OVERVIEW

SECURITY AND CONTINGENCY PLANNING

3.21.1 DEFINITION

Security is concerned with the protection of information and infrastructure against risks introduced through the acts of one or more human beings, either intentional or accidental.

Contingency planning is the development of a management plan that identifies alternative strategies to be used to ensure project success if specified risk events occur.

3.21.2 OVERVIEW

Over the last several years, the Department of Information Technologies (I.T.) has evolved from a mainframe-centric environment to an environment that is trying to keep pace in one of the fastest growing cities in the country. This evolution has included implementing several enterprise applications while increasing our user base to over 2,700 people. In addition to this evolution, I.T. has also increased its Internet presence to provide various services to the citizens of Las Vegas. I.T.'s evolution and phenomenal growth as well as our motto, "*Online rather than in line*" has caused a unique set of challenges in the information security area.

The information security program has had to change to meet these new challenges while providing a secure environment that ensures the integrity, availability and accessibility of information and systems. The security program is a risk-based program that uses a layered approach to the protection of resources. Whenever a change is planned, the risks to the existing infrastructure are assessed and only those security measures that address the risk are considered. This process provides risk-based controls at every level and ensures that each individual gets the accesses needed and nothing more.

At the network level, Cisco router controls and firewalls are used to protect internal resources from external non-trusted access. Access control lists are maintained and unnecessary ports and services are deactivated. I.T. has also created a DMZ ("Demilitarized Zone") as an additional safeguard that allows access to citizens and businesses without compromising the integrity of internal applications and databases. External traffic is monitored to protect against break-ins and attacks and additional protections are in place for electronic mail. E-mail is checked for worms and viruses and external messages with suspect attachments are quarantined until they can be reviewed for anomalies. If an incident does occur, an Incident Management Procedure is in place specifying appropriate responsive action.

SECURITY AND CONTINGENCY PLANNING

In addition to network level controls, I.T. also manages the access levels of authorized users via role-based controls. Every user of an application or system is provided only the access necessary to complete their authorized activities. Whether it is a citizen paying a parking ticket or attending Online Driver's Education, or an employee generating business licenses, each is allowed access to only information needed to complete that activity. Information Security personnel work with the client community, whenever a new application is planned, to develop these access-level profiles. These role-based access profiles ensure the integrity of the information in the systems while providing appropriate availability. Employees' activities are further managed via monitoring tools that will allow or disallow the users' ability to "Surf the Web" and provide spam control to reduce e-mail traffic and enhance the productivity of the workforce. An I.T. Access Procedure describes the steps for gaining access to the I.T. network and applications, and a User Account Termination Procedure specifies how user access ability is to be ended.

At the desktop level, I.T. ensures that virus checking is installed and activated on every machine and that policy does not allow users to install software or disable lockout features and virus updates. I.T. has a configuration control process for all applications and systems to ensure quality control is maintained. This quality control also provides an added level of protection while ensuring all software is appropriately licensed and managed. I.T. also has policies in place to control the ordering and installing of hardware and has standardized wherever possible.

This layered, risk-based approach has resulted in I.T. having an environment that is protected against attack and insider threat while maintaining spending and resource levels at below the national average.

Very few organizations understand the steps needed for true business continuity. Most organizations have a highly sophisticated emergency response plan and a very detailed disaster recovery plan that includes extensive lists of equipment and systems in some priority order. What they generally neglect in the business continuity cycle is the important middle step, contingency.

When an actual disaster occurs, these organizations may have no process in place to keep their critical processes operational until full recovery can be accomplished. If the disaster is a major one full recovery can take many months and without contingency processes in place, critical systems cannot be maintained. This can result in loss of business or revenue, public embarrassment and in many instances complete business failure.

SECURITY AND CONTINGENCY PLANNING

Other organizations spend millions on disk mirroring, instantaneous switchover and duplicate environments without considering their true contingency needs.

Many times being down for one business day is completely acceptable and there are few environments where every system is business critical. These organizations could easily recover from backup media without the massive costs.

In order to determine the city's contingency needs, I.T. created a Contingency Task Force with representatives from every department. That group of business process experts was then trained, at a high level, on business continuity. They were tasked to declare their critical processes and to determine how long those critical processes could be inoperable. The group was then tasked with prioritizing each of the critical processes. This gave I.T. the opportunity to determine what resources needed to be provided for contingency.

At the same time the contingency needs were being determined, several enterprise applications were being implemented. These applications needed test and development platforms during their implementation and as changes were being made. I.T. decided that those systems could also be used for contingency processing, thus saving the high monthly costs of the warmsite provider. To accomplish this dual purpose, I.T. put the test and development systems at a secondary location. This allowed the systems to be used on a daily basis for testing while always being available for contingency. The contingency site is being expanded as more e-commerce and enterprise systems are being placed into production.

The secondary location was sized for expansion and has the network infrastructure and emergency power to allow for standalone processing of critical systems if the outage is valley wide. Having test platforms that can also be used for contingency during a disaster allows I.T. to meet the current contingency needs of our customers and the citizens while keeping the costs at reasonable levels. Current plans include decentralizing some of the servers in the current Computer Room and moving them to the contingency location. Additionally, I.T. plans to add some redundancy and possibly mirroring to the contingency site, which will reduce the recover time and ultimately provide for instantaneous recovery for future e-commerce applications.

KEY I.T. GOVERNANCE FUNCTIONS

3.22 SERVICE LEVEL AGREEMENTS (SLAs)

FEATURED IN THIS SECTION

3.22.1 DEFINITION

3.22.2 OVERVIEW

3.22.3 ALTERNATIVE SERVICE PROVIDERS

SERVICE LEVEL AGREEMENTS (SLA's)

3.22.1 DEFINITION

I.T. Service Level Agreements are contractual arrangements between I.T. and sub-entities (departments or city offices) to reach objectives and/or to provide services at agreed levels of delivery and quality. Also, a service level agreement can be created between I.T. and commercial vendors, referred to as Alternative Service Providers (ASPs).

An SLA should contain a specified level of service, support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be provided and for what fee.

3.22.2 OVERVIEW

An SLA should contain a specified level of service, support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be provided and for what fee.
More recently, I.T. departments in major enterprises have adopted the idea of writing a service level agreement so that services for their customers (users in other departments within the enterprise) can be measured, justified, and perhaps compared with those of ASPs.

Some metrics that SLAs may specify include:

- What percentage of the time services will be available
- The number of users that can be served simultaneously
- Specific performance benchmarks to which actual performance will be periodically compared
- The schedule for notification in advance of changes that may affect users
- Help desk response time for various classes of problems
- Dial-in access availability
- Usage statistics that may be provided

SERVICE LEVEL AGREEMENTS (SLA's)

3.22.3 ALTERNATIVE SERVICE PROVIDERS

Alternative Service Providers, or ASPs, are commercial vendors that create, manage, and distribute software-based services and solutions to customers. In essence, ASPs are a way for entities to outsource some or almost all aspects of their information technology needs. They may provide software solutions for I.T. to administer to customers or directly service and support end users.

ASPs can be categorized as:

- Enterprise ASPs -- deliver high-end business applications (e.g., e-mail services).
- Local/Regional ASPs – supply a wide variety of application services for local government or businesses, in lieu of having the applications developed inhouse.
- Specialist ASPs -- provide applications for a specific need, such as Web site services or human resources.

As of February, 2005, the major ASP's delivering applications for the city are:

- Oracle, providing finance, payroll, and human resources software
- Hansen Information Technologies, providing for business services and building and safety applications
- Active Community Solutions, providing the Class software in use by the Department of Leisure Services

KEY I.T. GOVERNANCE FUNCTIONS

3.23 STRATEGIC PLANNING

FEATURED IN THIS SECTION

3.23.1 DEFINITION

3.23.2 OVERVIEW

STRATEGIC PLANNING

3.23.1 DEFINITION

Strategic Planning is the process of determining an organization's long-term goals and then identifying the best approach for achieving those goals.

3.23.2 OVERVIEW

Strategic planning at the City of Las Vegas begins with the plans worked out by city management to achieve the goals set by the elected City Council. Each year meetings are held between city management and departmental directors to have these goals precisely communicated and to discuss ways in which departmental operations can move to achieve them. Necessary funding is estimated as part of the budget process (see Budget Planning and Process) and combined with the funds necessary for operations already established. Then it is up to departmental middle management to communicate these goals to staff and to work out how they are actually going to be tasked and completed. Normal day-to-day operations continue alongside new special projects because an implicit and continuing goal of the City Council and city management is the smooth operation of city services provided to citizens.

I.T. is particularly involved because so many new strategic initiatives require information technology participation in some way.

KEY I.T. GOVERNANCE FUNCTIONS

3.24 SYSTEMS ADMINISTRATION

FEATURED IN THIS SECTION

3.24.1 DEFINITION

3.24.2 OVERVIEW

3.24.3 OPERATING SYSTEMS

3.24.4 HARDWARE

SYSTEMS ADMINISTRATION

3.24.1 DEFINITION

Systems Administration focuses on the planning, acquisition, implementation, and administration of the hardware and software comprising enterprise-wide networking and computer systems.

3.24.2 OVERVIEW

The City of Las Vegas Systems Administration group's primary objective is to ensure a secure and reliable enterprise computing environment that meets the current and future requirements of the organization while observing fiscal guidelines.

To achieve this objective, Systems Administration has developed the following goals:

- Ensure a secure network environment by implementing and enforcing industry-accepted computing security protocols at both the network edge and within the internal network.
- Ensure a secure server environment by implementing and enforcing a "best-practices" approach to computer security at both the operating systems and application software level.
- Evaluate, recommend, and implement enterprise network and computing solutions to support the operational and administrative requirements of the city.
- Advise management on current and emerging technologies and their effects on the city's computing and networking infrastructure.
- Coordinate inter-agency data-sharing requirements and processes.
- Develop short- and long-term plans for maintaining and improving the capacity of our enterprise systems infrastructure.
- Monitor systems' condition and performance to ensure peak efficiencies.

The systems group is greatly appreciated for researching, recommending, and implementing solutions "behind the scenes" to make the desktop and application environments run smoother for city staff. Examples where they are particular heroes involve their implementation of the Symantec virus detection system and Spam Sleuth's spam-blocking software.

SYSTEMS ADMINISTRATION

OPERATING SYSTEMS

As of April, 2005, several operating systems are deployed to serve varying environments.

Current CLV Operating Systems				April, 2005
Operating System	**Hardware Vendor**	**Hardware Bit Capacity**	**Applications Area**	**User Group**
TRU64 (Unix)	HP	64	Oracle applications	Finance, Human Resources (HR)
Solaris (Unix)	Sun	64/32	GIS	I.T. Systems staff
Unisys HMP	Unisys	64	Legacy systems	Municipal Courts, Detention
Microsoft Windows NT (Planned for retirement)	Dell	32	Pyramid (Workers Comp)	HR Insurance Services
Microsoft Windows 2000	Dell	32	Hansen Apps Servers Desktops	All
Microsoft Windows 2003	Dell	32	Servers	I.T. Systems staff
Microsoft Windows XP	Dell	32	Desktops	All
Macintosh OS	Apple	64	Graphic Arts Desktops	I.T. Graphic Arts Section
VMWare	Dell	32	Testing	I.T. Systems staff

The VMWare operating system supports software to create large virtual environments to use in testing.

SYSTEMS ADMINISTRATION

3.24.4 HARDWARE

As of February, 2005, over 100 servers are in use, with the majority located in the I.T. Computer Room located in the 5th Floor. Most of the servers are Dell, which are purchased and maintained via contracts. These run application systems, both purchased and developed in-house. Other types of hardware configurations are necessary to suit environments centered on specialized software. A Hewlett Packard (HP) GS128 server in the I.T. Computer Room runs the Oracle applications for Finance and Human Resources; it is backed up by an HP GS140 server located at the West Yard contingency site, over 10 miles distant.

A Unisys CS7101 server runs Unisys' HMP operating system, which supports both Microsoft Windows 2000 and the Unisys proprietary MCP (Master Control Program) operating systems. The MCP proprietary environment supports the legacy COBOL programs dedicated to Municipal Courts and Detention and Enforcement applications. It is backed up by a Unisys model LX6120 box configured similarly at the West Yard contingency site. New Dell models are added as necessary to handle increasing workloads as older machines are being retired, and this has been keeping the number of servers at just over 100.

KEY I.T. GOVERNANCE FUNCTIONS

3.25 TECHNICAL ARCHITECTURE

FEATURED IN THIS SECTION

3.25.1 DEFINITION

3.25.2 OVERVIEW

TECHNICAL ARCHITECTURE

3.25.1 DEFINITION

Enterprise Technical Architecture (ETA) describes the continually evolving blueprint that guides all aspects of an enterprise's technology life cycle. ETA is concerned with activities for the definition, purchase, creation, modification, integration, deployment, operation, and retirement of the infrastructure and supported applications. It is governed by both technical management and engineering practices in use throughout the enterprise.

3.25.2 OVERVIEW

The ETA defines the standard I.T. environment needed to support the enterprise's vision within the scope and time period established by City Council and the City Manager's Office, recognizing that this environment must be responsive to change.

The ETA is primarily concerned with enterprise-wide integration issues, describing the technology-related entities and relationships that need to be managed across the enterprise. Technology-related entities may include application platforms, software applications, information access and storage, networking, and the external and internal users of the applications. Relationships deal with the exchange of services across entity interfaces. The ETA constrains individual information system technology decisions when necessary to promote interoperability, integration, or other enterprise technology goals. As necessary, specific products are procured or developed to improve the operability of ETA elements. Approved projects are the means by which changes to the ETA are undertaken successfully.

The architectures guide, not dictate, as there is always room to negotiate based on immediate needs. The city may choose to constrain a department's design and fabrication options by selecting preferred vendors, products, or existing enterprise-provided infrastructure for the overall benefit of the enterprise. Often, constraints may arise due to existing I.T. inventories, such as decisions to keep existing applications or technology due to lack of funding. Certainly, having microcomputers inventoried and controlled centrally, as well as replaced according to a strict schedule, benefits the enterprise. The decision to use commercially available or existing products will influence the standards that are selected as the basis of the ETA.

TECHNICAL ARCHITECTURE

An enterprise can elect to absorb the risk of developing versus procuring in order to reduce the risk of vendor lock-in and associated maintenance fees; similarly it may be more advantageous to procure in order to reduce the considerably longer implementation schedule associated with development. These risks can be documented in the decisions affecting the selection of standards and products in the technical architectures. This helps determine whether the enterprise should adapt the business to a COTS system available in the marketplace, or incur the cost of developing an application inhouse. As of February, 2005, COTS applications are supporting finance, human resources, business services, building and safety, and leisure services.

Below is a chart showing how the various technical architecture components and those responsible are related in support of the enterprise:

Enterprise Architecture

	Type	**Who**	**What**	**When**	**Where**	**Why**	**How**	**Result**
View	*Model*	*Interface*	*Data*	*Time*	*Network*	*Reason*	*Function*	*Product*
Scope	Contextual	Planner	List of things important	List of events	List of locations	List of goals and strategies	List of processes to be performed	List of entity organizations affected
Enterprise	Conceptual	Owner	Semantic model	Master schedule	Logistics network	Business plan	Business process model	Work flow model
System	Logical	Designer	Logical data model	Processing structure	Distributed system architecture	Business rule model	Application architecture	People interface architecture
Technology	Physical	Builder	Physical data model	Control structure	Network architecture	Business rule design	System design	Presentation architecture
Detail Example (one of many)	Low level	Responsible staff	Data element or field	Event timing	Hub, router location points	Business rule specification	Application computer program	Security architecture diagram
Outcome	High level	User or citizen	Database	Schedule	Functioning network	Strategy	Application system	**Supported enterprise and citizenry**

The degree to which the elements within this architecture are utilized and documented for any application depends upon the size and complexity involved. The architects establish the essential characteristics that the technical architecture must promote and, as a result, decide how closely, or loosely, to follow the enterprise architecture model for each system.

TECHNICAL ARCHITECTURE

For example, scalability may be a concern (i.e., being able to increase throughput without significantly increasing cost per user or per transaction). If so the technical architecture chosen may include loosely-coupled, distributed technologies that have an inherent ability to scale, such as web-based solutions, as opposed to specifying a single, tightly integrated application supported by a large processing system.

Addressing technology from an enterprise standpoint enables all of the elements of a system to be considered in relation to one another, including interface points between contextual ideas, finished products, and the people involved.

SECTION 4 - I. T. GOVERNANCE-RELATED POLICIES, PROCEDURES, & GUIDELINES

4.1 AUDIO/VISUAL EQUIPMENT POLICY/PROCEDURE
4.2 COMMUNICATIONS EQUIPMENT POLICY
4.3 COMMUNICATIONS EQUIPMENT PROCEDURE
4.4 E-MAIL POLICY
4.5 E-MAIL RECORDS POLICY
4.6 INCIDENT MANAGEMENT PROCEDURE
4.7 INFORMATION RESOURCES USE POLICY
4.8 INTERNET POLICY
4.9 INTERNET PROCEDURE
4.10 INTERNET WEB SITE CONTENT MANAGEMENT POLICY
4.11 INTRANET POLICY
4.12 INTRANET PROCEDURE
4.13 INTRANET WEB SITE CONTENT MANAGEMENT POLICY
4.14 I.T. ACCESS PROCEDURE
4.15 ITCCC CHANGE REQUEST PROCEDURE
4.16 MICROCOMPUTER HARDWARE POLICY
4.17 MICROCOMPUTER SOFTWARE POLICY
4.18 PURCHASED SOFTWARE EVALUATION GUIDELINES
4.19 REPORT REQUEST POLICY
4.20 REPORT REQUEST FORM PROCEDURE
4.21 REPORTING MICROCOMPUTER PROBLEMS
4.22 SOFTWARE CHANGE CONTROL POLICY
4.23 SOFTWARE DEVELOPMENT LIFE CYCLE POLICY
4.24 SOFTWARE TESTING POLICY
4.25 SOFTWARE TESTING PROCEDURE
4.26 SOURCE CODE MANAGEMENT POLICY
4.27 USER ACCOUNT TERMINATION PROCEDURE
4.28 VERSION CONTROL POLICY
4.29 WEB SITE PRIVACY POLICY

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.1 AUDIO/VISUAL EQUIPMENT POLICY/PROCEDURE

4.1.1 PURPOSE

To establish policy and procedures by which I.T. will maintain state of the art audio/visual equipment to utilize in presentations of all kinds by both I.T. and other city departmental staff.

4.1.2 SCOPE

All city employees using I.T.-supplied audio/visual equipment and I.T. employees associated with its operation and placement.

4.1.3 OVERVIEW

In conjunction with efficient asset management, it is a matter of policy that I.T.'s audio/visual equipment will be shared with other departments. This document advises other departments as to where the equipment is kept, what is available, and the procedure for checking the equipment out and returning it. Also discussed is the need for making arrangements in advance if additional software or data are needed.

Employees utilizing this equipment are required to sign an agreement ensuring responsibility for care of the equipment during their period of use. No system reconfigurations by non-I.T. staff are permitted. Repair or replacement due to damages incurred during use will be charged back to the department having responsibility.

I.T. staff will assist with the presentation if the request is made sufficiently in advance so as not to cause conflict with other duties.

Reservation for conference room facilities required for presentations must be made with the Department of Human Resources.

4.1.4 AUDIO/VISUAL EQUIPMENT POLICY/PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

Audio/Visual Policy/Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.2 COMMUNICATIONS EQUIPMENT POLICY

4.2.1 PURPOSE

To set forth the policy that must be followed for using City of Las Vegas cellular phones, radios, pagers, and related communications equipment in conducting city business.

4.2.2 SCOPE

All employees. This policy applies to all cellular phones, radios, pagers, or related equipment in use or in stock by the City of Las Vegas. The policy covers all personnel to whom these devices are issued for conducting their city business as well as those employees charged with the administration and maintenance of this equipment. The policy also references employees charged with the supervision and administration of the employees to whom equipment is issued.

4.2.3 OVERVIEW

Specifically, this document covers policy issues relating to:

- Requesting a cellular phone, radio, pager, or related communications equipment
- Issuance of communications equipment
- Usage of communications equipment
- Returning communications equipment
- Reporting lost, stolen or damaged communications equipment
- Reporting malfunctioning communications equipment

Requests from non-I.T. staff for communication equipment must be made by responsible departmental staff to I.T. The requesting department is then billed a monthly fee by I.T. to recover procurement and usage costs during the period of departmental usage. Issuance requires that the employee utilizing the equipment reads both the Communications Equipment Policy and the Communications Equipment Procedure and sign to that effect. A key usage preclusion pertains to non-operation of cellular phones and headsets while driving motor vehicles.

Key points are covered in the policy regarding returning and transferring equipment, as well as how to report malfunctioning devices.

4.2.4 COMMUNICATIONS EQUIPMENT POLICY INTERNAL LINK

Intranet readers may access the document at:

Communications Equipment Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.3 COMMUNICATIONS EQUIPMENT PROCEDURE

4.3.1 PURPOSE

To set forth the procedures that must be followed for using City of Las Vegas cellular phones, radios, pagers, and related communications equipment in conducting city business.

4.3.2 SCOPE

All employees. This procedure applies to all cellular phones, radios, pagers, or related equipment in use or in stock by the City of Las Vegas. The procedure covers all personnel to whom these devices are issued for the purpose of conducting city business as well as those employees charged with the administration and maintenance of this equipment. The document also references employees charged with the supervision and administration of the employees to whom equipment is issued.

4.3.3 OVERVIEW

This document covers procedural issues relating to:

1. Requesting a cellular phone, radio, pager, or related communications device
2. Issuance of communications equipment
3. Usage of communications equipment
4. Returning or transferring communications equipment
5. Reporting lost, stolen or damaged communications equipment
6. Reporting malfunctioning communications equipment

COMMUNICATION EQUIPMENT PROCEDURE

The key positions of authority and usage as well as their responsibilities with regard to the procedure are listed initially. Specific services provided are outlined:

- Add, delete, or move: phone, FAX, and modem lines
- Add, move, change, or remove phones
- Add or delete voice mail
- Repair phone equipment or lines
- Replace or update cellular phones, radios, pagers, or related equipment no longer meeting needs of department
- Issue temporary cellular phones (less than 30 days)
- Issue cellular phones on permanent basis
- Order portable and vehicle radio equipment
- Order voice and digital pagers
- Order public address systems (office paging)
- Repair cellular phones
- Repair portable and vehicle radio equipment

How to go about requests for communication equipment are covered and the steps involved in issuance are described. During the period of communications equipment usage and operation, employees are reminded of key points to follow.

Requests must be made by responsible departmental staff to I.T. The requesting department is then billed a monthly fee by I.T. to recover procurement and usage costs during the period of departmental usage. Issuance requires that the employee utilizing the equipment reads both the Communications Equipment Policy and the Communications Equipment Procedure and sign to that effect. An important usage proclusion pertains to non-operation of cellular phones and headsets while driving motor vehicles.

Key points are discussed in the procedure regarding returning and transferring equipment, as well as reporting malfunctioning devices.

Employees are advised of the procedures to be followed for turning in communications equipment not only when departing the city's employment but when on leave in excess of 10 business days. Also covered is how to go about transferring equipment properly.

Specific actions are delineated when reporting lost, stolen, or damaged equipment during both day and evening shift hours. Finally, the procedures for reporting malfunctioning communications equipment are given

COMMUNICATIONS EQUIPMENT PROCEDURE

4.3.4 COMMUNICATIONS EQUIPMENT PROCEDURE INTERNAL LINK

Intranet readers can view the procedure at:

Communications Equipment Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.4 E-MAIL POLICY

4.4.1 PURPOSE

To set forth standards for access to, for use of, and for disclosure of electronic mail (e-mail).

4.4.2 SCOPE

All employees.

4.4.3 OVERVIEW

Users are reminded that they are not to transmit sensitive materials via e-mail nor send out harassing messages of any kind. While short personal messages are permitted, they must be sent and read on personal time.

Management reserves the right to have access to and view e-mail content at any time and to restrict or deny use of e-mail to any employee(s) at any time.

Specifically, e-mail is to be used for business purposes and not for:

- Personal gain
- Expressing personal opinion
- Supporting or advocating non-city-related business or purposes
- Intercepting or eavesdropping
- Soliciting, advertising, or promoting non-city business
- Copying and/or transmitting documents in violation of copyright laws

Users are instructed to be aware that being password-protected does not imply that e-mail is for personal, confidential use. Generally e-mail messages are temporary communications that may be discarded routinely; however, when an e-mail assumes the identity of a record, proper retention procedures apply.

E-mail maintenance and responsibilities are discussed, involving proactive saving and deletion by users and automatic deletion by the system according to date. Also covered is e-mail etiquette – including keeping e-mails brief, to the point, courteous, and professional. Having an e-mail in all-caps is considered by many to be equivalent to shouting and discourteous.

E-MAIL POLICY

4.4.4 E-MAIL POLICY INTERNAL LINK

Intranet readers may access the document at:

E-Mail Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.5 E-MAIL RECORDS POLICY

4.5.1 PURPOSE

To set forth a policy for managing electronic mail (e-mail) as records.

4.5.2 SCOPE

All employees.

4.5.3 OVERVIEW

Electronic mail, or "e-mail," is a tool used to transmit information between two or more parties via computers connected through a network. However, it is not correct to assume that every e-mail is to be treated as a public record. Many e-mails can be regarded as non-record transmittals that can be acted upon relatively quickly and then deleted. Public records are official city records not otherwise declared by law to be confidential.

This document is concerned with the treatment of e-mail as records. A separate document, E-Mail Policy, exists to cover the general use of e-mail.

4.5.4 E-MAIL TYPES

E-mails can be classified into four basic categories:

- Transitory Business Messages
- Personal Messages
- Duplicate Records
- Public Records

City employees using e-mail to transmit or receive information must be knowledgeable of their responsibilities with regard to public records. The difficulty is determining which e-mail contains information that should be considered to be a public record. In some cases, the classification of a message as a public record may differ between the sender and the receiver(s) because of the effect that the information may have on the message recipient(s). The confidentiality of a message really has nothing to do with whether it is a record or not. (The confidential aspect is fair warning to users that simply marking a record as 'Confidential' does not prevent it from becoming a public record, and 'public records' are the subject of this policy. Further, a confidential message must never be sent between parties, even if it is clearly designated as 'Confidential,' because the message may later be determined to constitute a public record. An example of a confidential message might be a manager instructing a supervisor on a particular course of action with regard to a disciplinary matter.

E-MAIL RECORDS POLICY

By separate policy, e-mail information is automatically deleted after 45 days during weekend purge actions conducted by staff within the Department of Information Technologies (I.T.). This includes e-mails that might have been originally intended as public records. Any information that needs to be preserved longer than 45 days must be saved into personal files by the recipient.

All information sent via e-mail must be prepared under the assumptions that:

- The information sent via e-mail is not confidential nor later could be determined to be confidential
- The targeted recipient may not be the final recipient
- The information sent may be determined to be, and subsequently maintained as, a public record by another party
- The information sent and received will be deleted automatically by the system in 45 days.

Because of e-mail distribution and potential redistribution, messages, and any inherent errors or inappropriate comments, can typically reach a much larger audience than the primary target. This fact, together with the knowledge that an e-mail may end up as a public record, requires that city employees take care to prepare e-mail messages as professional representations of their respective departments and the city overall. Re-reading a composed message before sending it is always advisable. Some important points to remember when constructing e-mails that may become public records are:

- Appropriate level of formality for the targeted, and possible additional, audience
- Correct spelling
- Correct grammar
- Correct punctuation
- Use of appropriate subject titles
- Use of appropriate salutations and closings, if e-mail is sufficiently formal
- Making sure attachments referenced in the text are, in fact, attached
- Exclusion of inappropriate comments or referenced material

4.5.5 E-MAIL ATTACHMENTS

Care must be taken to ensure that attachments to e-mail messages are treated as part of the record and stored or referenced appropriately. By separate policy, e-mail attachments cannot exceed a designated maximum size established by the E-mail Administrator within the Systems Infrastructure Management Division of I.T. Under special circumstances, this maximum size may be increased by application to the I.T. Support Desk.

E-MAIL RECORDS POLICY

4.5.6 TRANSITORY MESSAGES

Transitory messages are defined as business-related communications that do not set policy, establish procedures, set guidelines, document city business, certify a transaction, or become a receipt. The informal tone of transitory messages can be compared to telephone or hallway-type conversations that involve business topics. The information conveyed during these e-mail exchanges is typically of temporary importance and has a limited administrative value. While transitory messages may have some official context (such as a non-policy announcement), they are not part of a business transaction. Also, since drafts of documents circulated for comment or approval have not been finalized yet, these are considered transitory.

Transitory messages are considered non-records and may be deleted when no longer administratively useful.

4.5.7 PERSONAL MESSAGES

E-mail communications that have no bearing on city business are categorized as personal messages. These messages have become a replacement for phone calls in many instances when performing simple tasks such as asking for assistance or extending an invitation. When using e-mail in lieu of the telephone, however, city employees need to be aware that there is no guarantee of privacy or confidentiality for personal messages transmitted via e-mail since all messages are owned by the city and may be monitored, viewed, printed, or further distributed at any time by other city employees. While short duration personal messages are permissible via e-mail during work times, as are short personal telephone exchanges, lengthy personal exchanges are not appropriate for e-mail during business hours. Personal e-mail messages that cannot be composed or absorbed in a short time frame must be written and read on personal time.

Personal messages are not public records and may be deleted immediately after receipt.

4.5.8 DUPLICATE RECORDS

E-mail allows swift communication to many recipients at once with great ease. These copies may be distributed via e-mail for convenience and stored by recipients for reference. However, duplicate records are not to be considered official documents.

Duplicate records are not public records and may be deleted immediately.

E-MAIL RECORDS POLICY

4.5.9 PUBLIC RECORDS

Public records are defined as information and/or documents created or assimilated in the course of conducting public business that document the activities and business of public employees. An official city record includes any materials made or received by a city department or office and preserved as evidence of the organization, operation, policy, or any other activity of that group. Examples of documents that may be considered public records and generated as e-mail are:

- Policies and procedures
- Correspondence or memoranda related to official city business, exclusive of duplicates (Specific examples might be data pertaining to case files, or contract-related issues)
- Work schedules and assignments
- Agendas and minutes of meetings
- Documents that initiate, authorize, or complete a business transaction
- Final reports and recommendations

4.5.10 MAINTENANCE OF PUBLIC RECORDS

Public records must be retained for a period appropriate to their content, according to applicable record retention schedules. If there is doubt about the retrievability of an electronic record over the course of its lifespan, the record has to be printed and maintained in hard copy format. Public records originating as e-mail messages must be printed out and stored in paper format or moved to the proper electronic storage location before the 45-day time period expires. If the message is not considered a public record by the sender but is by the recipient, then the responsibility for maintaining a separate file location accessible to those affected lies with the recipient.

Permanent public records are archival records with legal, administrative, or historical value that must be retained indefinitely for use by future generations. Since no electronic medium exists, as of 2005, that fulfills this requirement to the satisfaction of records administrators, public records requiring permanent storage must be converted to paper, microfilm, or another medium considered acceptable for permanent records retention. Whenever an electronic medium emerges that can be regarded as permanent, this policy will be re-evaluated and updated.

4.5.11 E-MAIL RECORDS POLICY INTERNAL LINK

Intranet readers may access the document at:

E-Mail Records Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.6 INCIDENT MANAGEMENT PROCEDURE

4.6.1 PURPOSE

To establish the responsibilities and processes for the discovery, management, and reporting of information security-related events that may become incidents.

4.6.2 SCOPE

All employees. This procedure specifically applies to Department of Information Technologies personnel assigned the responsibility for incident management and response. It also applies to any organization that identifies an information security-related event.

4.6.3 OVERVIEW

This procedure is intended to ensure that:
- Information security-related events are reported in a timely manner.
- Necessary information is reported.
- Events are properly investigated.
- Appropriate follow-on activities (i.e., correction of system vulnerability, enhancement of system security) are accomplished after the event is discovered.

This procedure pertains to I.T. personnel assigned to incident management and response and to any city organization identifying a security-related event.

Specifically designated in this procedure are responsibilities for the:
- Director of I.T.
- The Information Security and Contingency Administrator (ISCA)
- I.T. Division Personnel
- The I.T. Support Desk
- Any employee involved in reporting an incident

Possible event sources are listed and employees are reminded that these occurrences must be investigated and reported. Monitoring of internally-accessed applications is specified as a means to provide information on misuse, fraud, or abuse by employees or other authorized application users. At the systems level, monitoring criteria are also discussed.

INCIDENT MANAGEMENT PROCEDURE

Employees are cautioned to understand the difference between an event (an occurrence requiring notification, investigation, and potential corrective action) and an incident (an information security-related event or activity that results in, or could result in, attempted, suspected, or actual compromise of information; or that results in the waste, fraud, abuse, loss, or damage of property or information).

Examples of 'events' are provided:

- Unauthorized access
- Theft
- Interruption to computer service
- Interruption to security controls
- A disaster such as fire, flood, explosion, or destruction
- Damage to equipment, data files, or computer programs
- Discovery of a vulnerability
- Disclosure of passwords, security controls, or protocols
- Unauthorized repetitive attempts to access system (external hacker)
- Unauthorized use of the system
- Viruses, worms, and Trojan Horses

Once an event becomes an incident, it needs to be ranked in terms of severity according to the following criteria:

Critical – Complete penetration of a system, penetration that exposes hardware and software vulnerabilities, physical loss that causes programmatic impact; known loss or compromise of sensitive information: discovery of a virus or worm that requires the shutdown of a critical process; or use of the system in any criminal or embarrassing way to the city.

Important - Loss or compromise of authentication mechanisms resulting in the suspected exposure of sensitive information; penetration of a sensitive system without allowing control of the system or access to all data; major misuse of a system by an authorized operator; downloading of inappropriate or illegal software or files; property destruction or theft; or suspected loss or compromise of sensitive information or security software features.

Routine - An external attempt to access a system with little potential for success; minor abuse of a system by authorized users; password loss or account sharing; downloading and installing screen savers and other items that could have a negative impact on the environment; or viruses and worms detected before entering the Wide Area Network (WAN)

INCIDENT MANAGEMENT PROCEDURE

The ISCA has the responsibility to ensure that information security-related events are analyzed and appropriate corrective actions are taken

Incident response and reporting will vary from event to event. In many cases, the infrastructure processes in place will automatically mitigate the event. Minimal information to be gathered by I.T. personnel during an event is listed as:

- Event Type
- Extent of event (single PC, LAN, mini computer, etc.)
- Source of event
- Potential recipients of infected material
- Steps taken (or planned) to mitigate the event

When a user reports an event, they are required to inform the I.T. Support Desk, and their supervisor or the ISCA. The person receiving information about the suspected event is required to contact the ISCA, who initiates the Incident Report. The ISCA then pursues getting the report investigated and completed, and then informs the Director of I.T. The Director of I.T. informs city management, if necessary. Additionally, steps to follow for vendor-reported and for internally-related events are provided.

When an event becomes an 'incident,' certain reporting thresholds are given, according to the following table:

Ranking	Reporting Time to ISCA	Reporting Time to Director
Significant	Within 2 hours	Within 4 hrs
Important	Within 8 hours	Within 24 hours
Routine	Within 7 days	Within 30 days

The Director of I.T. assumes responsibility for any corrective action, and the ISCA determines what corrective action is to be taken.

The ISCA is responsible for keeping audit trail records of all reported events and resulting corrective actions, and the Director of I.T. ensures that any recommended follow-up activities are completed prior to closing the report.

4.6.4 INCIDENT MANAGEMENT PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

Incident Management Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.7 INFORMATION RESOURCES USE POLICY

4.7.1 PURPOSE

To establish a policy for employee use of information-related resources provided by the city to facilitate job performance.

4.7.2 SCOPE

All city employees, elected officials, volunteers, vendors and other affiliates who use or access city-provided computing resources, regardless of their location.

4.7.3 OVERVIEW

The efficient use of information resources can improve the quality, productivity, and cost effectiveness of the city's work force. The purpose of this policy is to ensure proper use of these resources and govern user behavior pertaining to the usage of internal and publicly-accessible computer systems.

The rights and responsibilities of a user of city information resources are listed below. In order to use these resources properly, each new employee must understand and agree to these responsibilities and acknowledge their agreement by signing an "Information Technologies Request Form." Existing users are responsible for keeping these ideas in mind through this policy. Specific areas to consider are listed below.

- Internet - Except for limited personal use during approved breaks, lunch and non-work hours, the Internet should be used for official city business only. Access to the Internet requires authorization from a Director or an approved designee.
- Long Distance - It is the Policy of the city to use long distance for the conduct of city business. If anyone makes personal long distance calls for any reason, they must reimburse the Treasurer for the amount of each call.
- Confidentiality - It is the Policy of the city to protect the confidentiality and integrity of its information. Disclosure and discussion of confidential information obtained from departmental records is a violation of Policy. Violation by employees, staff, or contractors may constitute grounds for corrective action up to and including termination of employment or contract. Unauthorized release of confidential information may also have personal, civil, and/or criminal liability and legal penalties.

INFORMATION RESOURCES USE POLICY

- Compliance **-** Compliance with this document lies with the User's immediate supervisor/ manager and ultimately the User's Department Director. Failure to comply with the requirements of this document and information resource policies and procedures can lead to the revocation of system privileges and/or disciplinary action up to and including termination.
- Monitoring - Whenever someone uses city computer resources or is connected to city systems, the IT staff has the right to monitor and control any and all aspects of this usage. This includes, but is not limited to, stopping running programs, removing or compressing files, or in cases in which there is a reasonable cause for suspicion and with explicit approval of management, the right to examine the contents of files and electronic mail. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of information resources.

Users are entitled to use their computer account only as long as they are an employee or approved volunteer or contractor. Specific "Do's" and "Don't's" regarding usage are spelled out below.

- Passwords must be protected, kept secret and not shared with other people. Users are not allowed to use another person's account with or without their permission.
- City E-mail services must be used for official business only.
- Although the Internet can be accessed for personal use, users cannot conduct activities that would be potentially embarrassing to the city. This includes but is not limited to; contact with web sites or downloading of any material which would be reasonably recognized as sexually oriented, violent, profane, or extremist; use that would incur any unauthorized expense for the city; or use involving gambling or game playing.
- Individuals cannot conduct or manage a personal business using city resources.
- The city strictly adheres to all software vendors' license agreements. When at work or when using city networking resources, users must not copy software in a manner that is not consistent with a vendor's license.
- Users must not reproduce copyrighted material posted or otherwise available from external sources or over the Internet without the permission of the author/owner.
- Individuals must not access, download, or exchange pirated software, games, purloined passwords, or any other inappropriate material.
- Users must conduct all communication in a professional manner consistent with the same standards as formal letters.
- Systems will automatically scan all software downloaded from external sources such as the Internet for viruses. Users accessing city systems from outside the WAN must ensure the system they are using to access the WAN has virus software installed with up-to-date definitions and is at the highest possible patch level.

INFORMATION RESOURCES USE POLICY

- Supervisory and IT Department approval is required before any software can be installed.
- Users must not send or receive any sexually oriented messages or images.
- Individuals must not place city-owned or leased software, internal memos, or other information on any publicly accessible system unless approved by management.
- Users must not access or transfer electronic mail from unapproved external mail services. Mail received from these services could contain viruses, Trojan horses or other code that could result in infection of city systems.
- The Support Desk must be immediately notified of any changes in the user's organization or employment status so appropriate action may take place regarding their accesses.

4.7.4 INFORMATION RESOURCES USE AGREEMENT LINK

All of the material contained in the agreement form of this document is contained here. However, Intranet readers may access the Information Resources Use Agreement document at:

Use of IT Resources

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.8 INTERNET POLICY

4.8.1 PURPOSE

To establish a policy for using the publicly-accessible Internet and for posting to the City of Las Vegas Web Page.

4.8.2 SCOPE

This document pertains to city elected officials, employees, volunteers, or other affiliates utilizing or posting to the city-provided Internet facilities. The policy also references employees charged with the supervision and administration of the employees accessing the Internet or performing website authoring.

4.8.3 OVERVIEW

The goal of providing Internet services is to improve the quality, productivity, and general cost effectiveness of the work force. Internal users must fill out and submit the IT Request Form posted on the internal Intranet when seeking access to the Internet while at work.

Department directors are advised of their roles in ensuring that information posted on the city's website is accurate and timely. Even though each department has their own message, it is up to the Office of Communications to monitor and enforce consistency. For any information provided on the Internet from a city database, it is the responsible department's responsibility to implement appropriate safeguards that balance the availability of public information with citizens' right to privacy. For example, providing specific identification information to the Internet would allow a citizen to pay a parking citation online but would not allow someone to use the Internet to discover the parking violation habits of others. Also, the providing Department must not post on the Internet elements from records that might be considered sensitive, such as business financial information.

The city reserves the right to monitor all Internet use as well as stored information created or received with the city's information systems without notice. This helps to ensure that public resources are being used for appropriate purposes and that the city's information systems are operating as efficiently as possible.

INTERNET POLICY

Department directors are authorized to restrict or allow limited personal use of Internet browser access within their departments. This must be conducted only on an employee's personal time during the scheduled lunch break or after hours.

Inappropriate uses are listed, including incurring unauthorized expenses, gambling, seeking outside employment or a commercial purpose, downloading unauthorized software, and contacting or downloading from sites that might be embarrassing to the city. Also prohibited is use of city property for political activities, in accordance with a municipal code.

City of Las Vegas websites are precluded from endorsing or providing favorable treatment to persons, organizations, or business enterprises unless approval is given by the Office of Communications. When an outside link is approved, an appropriate disclaimer notifying the User that they are leaving the city's website shall be required.

Software is prohibited from being downloaded and/or installed from any source without written approval from I.T. I.T. may direct that the material be scanned for viruses prior to installation.

Users are not permitted to subscribe to any list servers or mailing lists without obtaining prior written approval from I.T.

4.8.4 INTERNET POLICY INTERNAL LINK

Intranet readers may access the document at:

Internet Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.9 INTERNET PROCEDURE

4.9.1 PURPOSE

To establish procedures for use of and posting to the publicly-accessible Internet computer network.

4.9.2 SCOPE

This document pertains to city elected officials, employees, volunteers, or other affiliates utilizing city-provided Internet facilities or creating Internet website material. The procedure also references employees charged with the supervision and administration of the employees performing Internet access or website authoring.

4.9.3 OVERVIEW

This document begins by reminding users that they are responsible for their use of Internet resources and that they are required to sign the Use of I.T. Resources Document available on the internally-based Intranet before they can gain access.

The Office of Communications controls Internet publishing at the citywide level and monitors the material posted by contributing departments for consistency.

Those developing Internet applications giving citizens access to information in city databases must:

- Implement appropriate safeguards to allow access while protecting citizen right to privacy.
- Not publish confidential information, such as business financial data.
- Invoke processing methods that encrypt sensitive information such as credit card numbers.
- Provide a disclaimer listing the personal data collected, its purpose, and disposition.

INTERNET PROCEDURE

When using Internet services, city employees should:

- Limit the use of Internet services to city business. Department Directors may authorize limited personal use outside of scheduled work hours.
- Never release confidential information in city databases without proper business justification.
- Never share information in city databases without prior written management approval.
- Not expect Intranet or Internet services to be confidential or private.
- Expect all data, including any that is stored or data printed as a document, to be subject to review or audit.
- Understand that the city reserves the right to monitor all Internet, and Intranet use, any other computer transmissions, as well as any stored information created or received by employees with the city's information systems. All Internet contacts are recorded and reports provided for management review.
- Remember that no system is 100% secure and that message confidentiality may be compromised.
- Cooperate with any investigation regarding the use of city computer equipment authorized by the employee's supervisor or the Department Director.
- Never download files or images from unfamiliar Internet sites.
- Never download copyrighted material without permission of the copyright holder, except to the extent allowed by fair use.

INTERNET PROCEDURE

When sending or receiving information via the Internet, employees are to consider the following points:

- Conduct business in a professional manner and remember that they are representing the City of Las Vegas.
- Do not place City of Las Vegas software, memos, or other information on any publicly-accessible Internet computer or website, including those privately owned, unless the posting of these materials has first been approved by the Office of Communications. In Internet correspondence, do not state as "city positions" those that are not officially endorsed by the city.
- Do not make statements that imply that the employee is officially speaking on behalf of the city.
- When using information from an Internet site for strategic city business decisions, verify the integrity of that information. Two points to consider are:
  Is the site updated on a regular basis? The lack of a revision date might indicate out-of-date information.
  - Is the site a valid provider of the information the employee is seeking?
- Carefully consider, before transmitting, the necessity of sending any confidential records over the Internet.

Employees are also informed that they must contact the I.T. Support Desk and seek I.T. approval before downloading any software via the Internet. I.T. may then determine whether or not the software needs to be scanned for viruses.

4.9.4 INTERNET PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

Internet Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.10 INTERNET WEB SITE CONTENT MANAGEMENT POLICY

4.10.1 PURPOSE

To establish a policy for employing a Web site content management system to ensure uniform Internet Web site standards, while providing independent departmental publishing for web-based information.

4.10.2 SCOPE

All employees associated with Internet Web site maintenance

4.10.3 OVERVIEW

This document directs the city to "implement efficient and effective processes to ensure that the look and feel of the City of Las Vegas Web site, www.lasvegasnevada.gov, remains consistent and timely." The city's Web site is a large site consisting of thousands of pages, and maintenance of the site is time consuming and complex. The Hypertext Markup Language, or HTML, used to create the Web site is difficult for non-Information Technologies (IT) professionals to learn and has to be carefully manipulated by dedicated IT staff. The city has implemented a system to allow non-IT staff to efficiently and effectively manage web content without HTML knowledge
.
Intranet content management is discussed in a separate policy.

4.10.4 CONTENT MANAGEMENT SYSTEM

A content management system (CMS) is used to provide an easy method to manage the Web site content and layout. A CMS allows non-technical content authors to create, edit, manage and post Web content in a timely manner. The oversight of the Web site and use of a CMS is done through a collaborative effort among several different departments. Jointly, the Office of Communications and IT provide authorization and access to the content management system. Authorization and access permits web content to be created, edited, deleted, restored, viewed and published.

INTERNET WEB SITE CONTENT MANAGEMENT POLICY

4.10.5 I.T.-MANAGED STANDARDS

I.T. Web site administrators are charged with establishing standards for individual web pages and the overall system in order to maintain a consistent look and feel for the entire city Web site. These standards can include layout, font size, background color, etc. Any deviation from the CMS must be approved through the IT and Communication departments.

4.10.6 SECURITY

I.T., using the CMS, assigns authorizations to each departmental user such that updates can only be made to the areas for which each user is responsible. The content management system requires password entry to control access.

4.10.7 PRIVACY

The city may collect certain information which may be considered personal. The information collected is subject to the same controls and uses outlined in the access and confidentiality provisions of the City of Las Vegas, State of Nevada, and Federal laws. Additional information on this subject may be found in the city's Web Site Privacy Policy.

4.10.8 CONTENT STANDARDS AND APPROVAL

Additions, changes and deletions to the Web site are controlled by a workflow component that is inherent in the content management software. All Internet content alterations by department content contributors flow to their respective managers for approval and to provide quality assurance. The Office of Communications is ultimately responsible for Internet Web site content. The workflow of the content management system is configured so that all content is reviewed by the Office of the Communications for grammar style/usage and content consistency before being released to the live Web site. The Office of Communications provides timely review and posting of departmental web content.

There are limited situations, as determined by the Office of Communications, when a particular department will be given authorization to post directly to the Web site via the CMS, bypassing review by the Office of Communications.

INTERNET WEB SITE CONTENT MANAGEMENT POLICY

4.10.9 BENEFITS

After implementation of a web CMS, those involved in web activities achieve the following benefits:

- Maintain consistency with Web site standards and design while requiring less attention from IT technical staff.
- Improve of Web site content by reducing publishing time.
- Increase user involvement in Web site publishing throughout the city.
- Improve readership by providing more up-to-date information on a 24-hour-per-day basis.
- Minimize demands on the IT web support effort by encouraging and empowering non-technical users to publish information to the Web site.

4.10.10 INTERNET WEB SITE CONTENT MANAGEMENT POLICY INTERNAL LINK

Intranet readers may access the document at:

Internet Web Content Management Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.11 INTRANET POLICY

4.11.1 PURPOSE

To establish a policy for using the internal, employee-accessible Intranet.

4.11.2 SCOPE

This document pertains to city elected officials, employees, volunteers, or other affiliates utilizing city-provided Intranet facilities or creating Intranet website material. The policy also references employees charged with the supervision and administration of the employees performing Intranet access or website authoring.

4.11.3 OVERVIEW

The goal of providing Intranet services is to improve the quality, productivity, and general cost-effectiveness of the work force. Users must request access to the computer systems and network by filling out and submitting the IT Request Form. The Department of Information Technologies (I.T.) will provide Users access to the operating system and internal network, which will automatically provide access to the Intranet.

The content of Intranet-based website pages must be approved by the Department Director or a designee.

Employees should not expect Intranet services to be confidential or private. All data, including any that is stored or data printed as a document, is subject to review or audit without notice. Also, employees must consider that no system is 100 percent secure and that the city reserves the right to monitor all Intranet use without notice.

The Intranet may serve as a tool for the dissemination of information to employees but is not intended to officially represent the city to others. The Intranet may permit the posting of personal material, such as items for sale, but only on designated website pages and in accordance with the policy specific to this application. Use of the Intranet for political purposes is prohibited in accordance with a city municipal code.

The city Intranet websites are not to endorse nor provide favorable treatment to any person, organization, or business enterprise, without management approval. When an outside link is approved, an appropriate disclaimer notifying the User that they are leaving the city's website shall be required.

INTRANET POLICY

4.11.4 INTRANET POLICY INTERNAL LINK

Intranet readers may access the document at:

Intranet Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.12 INTRANET PROCEDURE

4.12.1 PURPOSE

To establish procedures for using the internal, employee-accessible Intranet.

4.12.2 SCOPE

This document pertains to city elected officials, employees, volunteers, or other affiliates utilizing city-provided Intranet facilities or creating Intranet-based website material. The procedure also references employees charged with the supervision and administration of the employees performing Intranet access or website authoring.

4.12.3 OVERVIEW

User responsibilities are outlined first. Department directors are requested to approve department-specific Intranet-based material prior to posting on departmental web pages.

Employees are instructed to:

- Limit use of Intranet services to city business, with the exception of the city's Bulletin Board.
- Not expect Intranet services to be confidential or private.
- Expect all data, including any that is stored or data printed as a document, to be subject to review or audit.
- Understand that the city reserves the right to monitor all Intranet use, any other computer transmissions, as well as any stored information created or received by employees with the city's information systems.
- Remember that no system is 100% secure and that message confidentiality may be compromised.
- Cooperate with any investigation regarding the use of city computer equipment authorized by the employee's supervisor or the Department Director.

4.12.4 INTRANET PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

Intranet Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.13 INTRANET WEB SITE CONTENT MANAGEMENT POLICY

4.13.1 PURPOSE

To establish procedures for maintaining Web site standards while providing independent departmental publishing for web-based information.

4.13.2 SCOPE

All employees associated with Intranet Web site maintenance

4.13.3 OVERVIEW

This policy directs the city to implement "efficient and effective processes to manage the city's Intranet Web site." Web site management for large sites can be complex and time-consuming. The Hypertext Markup Language, or HTML, used to create the Web site is difficult for non-Information Technologies (IT) professionals to learn and has to be carefully manipulated by dedicated IT staff. Implementation of a content management system enables the separation of the page layout, navigation directions, and content functions so that the responsible departments can manage the web site content and IT technical staff can oversee the web site layout and routing functions.

Internet content management is discussed in a separate policy.

4.13.4 CONTENT MANAGEMENT SYSTEM

Web sites are categorized into two basic types:

1. Static, meaning content is:
   - Stored in HTML pages
   - Maintained only by IT web professionals
   - Easy to corrupt because of complexity
   - Subject to long wait time before changes can be addressed
   - Likely to become stagnant because changes are not made routinely
2. Dynamic, meaning content is:
   - Stored in a database
   - Maintained by non-IT departmental staff
   - Easy to update without technical knowledge
   - Easy to change quickly without prior notice to IT technical staff
   - Likely to remain current and interesting because of ease of maintenance

INTRANET WEB SITE CONTENT MANAGEMENT POLICY

Dynamic Web sites are attainable with the implementation of a commercial Web site content management system that uses software to interface data-based departmental information with IT-managed HTML web pages. The oversight of the Intranet Web site and use of a content management system are accomplished by IT Web site administrators and departmental content contributors working together. Authorization and access to the content management system are provided by IT such that web content can be created, edited, deleted, restored, viewed, and published.

4.13.5 IT-MANAGED STANDARDS

IT web site administrators are charged with establishing standards for individual web pages and the overall system in order to maintain a consistent "look and feel" for the city's Intranet Web site. These standards can include layout, font size, background color, etc. Maintaining a consistent appearance is easier to control when page layout is separated from page content as in a content management system. Any deviation from the Intranet content management system requires approval from IT.

4.13.6 DEPARTMENT-MANAGED CONTENT

Departmental users are assigned user privileges by IT web administrators in order to allow users to keep their particular content contribution to the Web site up to date. User privileges permit web content to be created, edited, deleted, restored, viewed, and published. The content can be text, graphics, multimedia, or a combination.

4.13.7 SECURITY

The IT Department, using the Intranet Web Site Content Management System, assigns authorizations to each departmental user such that updates can only be made to the areas for which each user is responsible. The Intranet Web Site Content Management System requires password entry to control access.

INTRANET WEB SITE CONTENT MANAGEMENT POLICY

4.13.8 CONTENT APPROVAL

Additions, changes, and deletions to the Intranet Web site are controlled by a workflow component that is inherent in the content management software. All Intranet content alterations by departmental users flow to their respective managers for approval and to provide quality assurance. Then, Intranet changes are released to the system for posting, since each department is responsible for its own Intranet content. Emergency posting of information, however, will not require review.

4.13.9 BENEFITS

After implementation of an Intranet Web Site Content Management System, those involved in web activities achieve the following benefits:

- Avoid growth in the IT web support effort by encouraging and empowering non-technical users to publish.
- Reduce risk of losing readers because of outdated web content.
- Improve readership by providing more up-to-date information on a 24-hour-per-day basis.
- Enforce compliance with Web site standards while requiring less attention from IT technical staff.
- Reduce turnaround publishing time for users significantly.
- Increase user involvement in Intranet Web site publishing throughout the city.

4.13.10 INTRANET WEB SITE CONTENT MANAGEMENT POLICY INTERNAL LINK

Intranet readers may access the document at:

Intranet Content Management Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.14 I.T. ACCESS PROCEDURE

4.14.1 PURPOSE

To establish access procedures for areas under the control of the Department of Information Technologies (I.T.) including but not limited to the City Hall Complex wiring closets, the City Hall 9th floor offices, the Computer Room and the West Service Center Contingency Site.

4.14.2 SCOPE

All employees and non-employees requiring long-term access and short-term access into IT-managed areas.

4.14.3 OVERVIEW

The document begins by delineating responsibilities for I.T.; the Department of Detention and Enforcement; the I.T. designee(s) given the responsibility as liaison between employees, visitors, vendors requiring access to IT-managed areas, and the Detention & Enforcement Access System Administrator; and employees charged with granting access to secure I.T. areas.

The employee requesting access to I.T.-controlled facilities must have their division manager submit the request to the I.T. Designee, who will then forward the approved request to the Department of Detention and Enforcement Access Systems Administrator for access activation. When an employee no longer needs access to these areas, the same process of notification is followed to affect access deactivation.

Visitor identification cards are required for non-city employees and an approval process similar to the one above is outlined, with the I.T. Designee issuing the I.D. card to the visitor. Cardholders are reminded of their responsibilities in ensuring that unauthorized personnel are not permitted into I.T.-controlled sites and that additional required non-city staff completes the access approval procedures specified.

If cards are lost or stolen, the Division Manager, I.T. Designee, or employee supervisor must notify the Department of Detention and Enforcement Access Systems Administrator so the cards can be deactivated.

If the visitor requirement is short-term, then an access card is not required, but the visitor must be escorted during the duration of the visit.

I.T. ACCESS PROCEDURE

4.14.4 I.T. ACCESS PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

IT Access Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.15 I.T. CONFIGURATION CONTROL COMMITTEE CHANGE REQUEST PROCEDURE

4.15.1 PURPOSE

To establish procedures necessary to bring a request for configuration control change (software, hardware, or operations) to a production environment before the Information Technologies Configuration Control Committee (ITCCC).

4.15.2 SCOPE

All employees.

4.15.3 OVERVIEW

New hardware, new versions of operating systems and applications software are periodically being integrated into operational systems. The function of the ITCCC is to determine that adequate testing has been performed and the change deployment is sufficiently planned and coordinated to make it successful. Some examples of change requests requiring ITCCC approval are listed as:

- Application system implementations and updates, whether inhouse-developed or purchased
- Operating system updates/new versions (server and desktop)
- New batch programs updating application database tables (including one-time updates)
- New server models
- New desktop equipment
- New network equipment models not used previously
- New enterprise, networked peripheral models
- New specialized interfacing equipment and software (such as to produce ID badges, etc.)
- Changes to procedures or operations

The steps for filling out an I.T. Configuration Control Request Form are given and the steps to be followed in the procedure are outlined and described. Also discussed are procedures for having special circumstances requests considered and approved via e-mail voting. Managerial approval (brief Intranet review of documentation covering testing and one member's recommendation and approval) is also provided.

I.T.C.C.C. CHANGE REQUEST PROCEDURE

4.15.4 I.T.C.C.C. CHANGE REQUEST PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

IT Configuration Control Committee Change Request Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.16 MICROCOMPUTER HARDWARE POLICY

4.16.1 PURPOSE

To set forth the policy to be used in the specification and purchasing/leasing of microcomputer systems.

4.16.2 SCOPE

All employees.

4.16.3 OVERVIEW

The City of Las Vegas purchases or leases microcomputer systems through contract vendors. These systems are acquired in order to meet the needs of city staff in the performance of their assigned duties.

It is the policy of the City of Las Vegas to procure the most current and economical microcomputer systems that satisfy the needs of the users and adhere to established standards for performance, quality, and reliability.

Microcomputer hardware is defined as all parts of the microcomputer system, including, but not limited to, the central processing unit, motherboard, interface boards, memory, keyboard, mouse, mass storage units (hard and floppy drives, tape units, etc.), video monitors, printers, and modems.

The Microcomputer Standards Committee sets the standards for microcomputer hardware. The committee determines the specifications for each microcomputer purchase/lease contract to include the computer equipment, network equipment, and systems software required to meet the needs of the users. Exceptions to the standards will be evaluated by the committee on an individual need basis and granted for true need only.

Each department will budget for the acquisition of new microcomputer hardware during the normal budgetary process. The Department of Information Technologies Department (I.T.) provides estimated costs of standard configurations to the Finance and Budget Division of Finance and Business Services for inclusion in the budget manuals. Departments may ask I.T. for estimated pricing of non-standard microcomputer configurations.

MICROCOMPUTER HARDWARE POLICY

All microcomputer hardware acquired by the City of Las Vegas must be purchased or leased through I.T. Hardware acquisition channels are restricted to ensure that the city has a complete record of all hardware that has been purchased or leased and that the hardware purchased or leased conforms to Microcomputer Standards Committee standards for performance and compatibility. Additionally, a single acquisition channel allows for multiple purchases at substantial discounts. A key policy provision is that hardware may not be purchased by any department other than Information Technologies using alternative payment mechanisms, such as city-sponsored credit cards, petty cash, or city procurement cards.

When hardware is received, it must be delivered first to I.T. in order to complete warranty registration and inventory requirements. I.T. staff is responsible for completing the warranty registration card and returning it to the manufacturer. Hardware must be registered in the name of the city and the department in which it will be used. Because of personnel turnover, hardware should never be registered in the name of the individual user. I.T. maintains a register of all of the city's hardware. The register contains:

- The date and source of hardware acquisition
- The location of each installation as well as the serial number of the hardware.
- The serial number of the hardware

After the above inventory and warranty registration requirements above have been met, the hardware must be installed by the I.T. Infrastructure Management Division staff. Manuals, tutorials and other user materials which came with the system are provided to the user. Only Information Technologies Department personnel may relocate microcomputer equipment, and will fully document equipment locations after installation or relocation.

Specific issues regarding home use and laptop security are also discussed.

Notebook computers, PDAs (Personal Digital Assistants), and PDA Combination Devices are provided to enable users to work away from their city offices. Approval for use of these devices must be granted in writing by the individual's department director on the Information Technologies Request Form (available on the Intranet). In order to ensure proper tracking of these assets and minimize possible loss, these assets must be documented in the IT inventory control system. Mobile computing devices may be provided based on business need justification and require the approval of the Department Director.

Periodic audits must be conducted in conjunction with the City Auditor's Office.

MICROCOMPUTER HARDWARE POLICY

4.16.4 MICROCOMPUTER HARDWARE POLICY INTERNAL LINK

Intranet readers may access the document at:

Microcomputer Hardware Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.17 MICROCOMPUTER SOFTWARE POLICY

4.17.1 PURPOSE

To set forth the policy to be used in the specification and purchasing/leasing of microcomputer systems software in order to prevent copyright infringement and to protect the integrity of the computer environment from virus threats.

4.17.2 SCOPE

All employees.

4.17.3 OVERVIEW

The city's Microcomputer Standards Committee appoints a Software Administrator from within its ranks who is charged with the responsibility for, and issued the authority for, enforcing this policy.

City of Las Vegas employees may not duplicate any licensed software or related documentation for use either on city premises or elsewhere unless the City of Las Vegas is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of software may subject employees and/or the city to both civil and criminal penalties under the United States Copyright Act.

Employees may not give or loan city-licensed software to anyone. City of Las Vegas employees may use software on local area networks or on multiple machines only in accordance with applicable license agreements.

Each new City of Las Vegas employee must complete a software education program which is included in the new employee orientation briefings. The Software Administrator is responsible for supplying the content of the program to the Department of Human Resources. Employees must sign an attendance list, which is kept on file. For existing employees, each city department distributes copies of this policy and collects the signatures of those who have read it. Attendance and reading lists are be used to document employee's familiarization with this policy.

MICROCOMPUTER SOFTWARE POLICY

When planning for hardware acquisition, software and training must be budgeted at the same time. When purchasing software for existing computers, such purchases must be charged to the department's budget for information technology (or appropriate budget that is set aside for tracking software purchases). Large license group purchases may be charged to the I.T. Infrastructure Management Division budget.

To purchase software, employees must obtain the approval of their supervisor, division manager, or department director and then follow established city procedures for the acquisition of computer software. Where the Microcomputer Standards Committee has established a program-type standard (e.g. Microsoft Word for word processing), that software will be purchased. Exceptions to the standard may be requested through the Microcomputer Standards Committee. Exceptions will be granted based on specific needs of the user not fulfilled by the standard software, to maintain uniformity of software within a work group, and other such unique circumstances. NRS 332 and city procurement policy do not allow personal preference as a valid reason for exception.

All software acquired by the City of Las Vegas must be purchased through the Department of Information Technologies. Software acquisition channels are restricted to ensure that the city has a complete record of all software that has been purchased for city computers and can register, support, and upgrade such software accordingly. Additionally, a single acquisition channel allows for multiple-license purchases at substantial discounts. Software may not be purchased through employee corporate credit cards, petty cash, field purchase orders, direct payment authorization, or travel and entertainment budgets.

The Software Administrator is responsible for completing registration and inventory requirements. Software must be registered in the name of the city and department in which it will be used. Because of personnel turnover, software should never be registered in the name of the individual user. The Software Administrator shall maintain a register of all of the city's software and shall keep a library of software licenses. The register must contain:

- The location of each installation as well as the identification number of the hardware on which each copy of the software is installed.
- The name of the authorized user (department/division/function)
- The software product's serial number (if applicable)

MICROCOMPUTER SOFTWARE POLICY

After the registration requirements above have been met, the software may either be installed by the I.T. Infrastructure Management Divsiion staff, an Information Technologies Coordinator, or a responsible representative in the end-using department. Manuals, tutorials and other user materials received with the software are provided to the user. Original diskettes must be kept in a safe storage area maintained by the Software Administrator. Copies of licensed software may be securely stored at designated remote sites for emergency use, with permission and direction of the Software Administrator.

Software no longer required must be reported or returned to the Software Administrator for redistribution or disposal. End users may not relocate software from one computer to another without coordination with the Software Administrator.

City of Las Vegas computers are government assets, and all software used must be legal and virus free. Only software purchased through the procedures outlined above may be used on city computers. Employees are not permitted to bring software from home and load it onto city computers. City-purchased software cannot be taken home and loaded on an employee's computer or copied for personal use.

It is important to understand the difference between freeware and shareware and to be aware that it is city policy to pay for copyrighted shareware software. Freeware can only be acquired and installed if approved by the Department of Information Technologies. Screen savers and font packages are also usually copyrighted products and may not be distributed freely.

Since computers are not to be utilized for entertainment purposes, games are inappropriate. It is the city's policy to remove games included with Microsoft Windows products before distribution.

I.T. staff assists the City Auditor's Office in performing periodic audits of software installed on city personal computers.

I.T. monitors the program content of all city microcomputer systems. Such monitoring is in addition to the periodic audits described above. The staff may use software metering programs, software management tools, visual inspection, and other means to ensure that only properly approved and licensed software resides on the city's systems. Unlicensed and unapproved software must be immediately removed from the computer.

MICROCOMPUTER SOFTWARE POLICY

4.17.4 MICROCOMPUTER SOFTWARE POLICY INTERNAL LINK

Intranet readers may access the document at:

Microcomputer Software Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.18 PURCHASED SOFTWARE EVALUATION GUIDELINES

4.18.1 PURPOSE

To provide guidelines to assist those in positions of authority in evaluating software packages and their provider corporations prior to authorizing software purchases.

4.18.2 SCOPE

City management, Director of Information Technologies, department directors, and their designees

4.18.3 OVERVIEW

The City of Las Vegas, City Council, and city management are responsible for ensuring that resources are available to properly evaluate the risks and control issues of purchased software and vendor companies prior to purchase.

These guidelines are recommended for significant software purchases or when the software will support a critical aspect of the city's operation. The recommended practices identify the type of studies or analyses that should be performed to improve the evaluation process and reduce the risk of the software not meeting the needs of the City of Las Vegas. In cases where there are limited alternatives for purchasing software such as single vendor applications, or operating system software designed for selected manufacturer's hardware, portions of the guidelines may not be applicable.

It is appropriate to analyze user requirements before evaluating vendor software packages. This analysis should define the business reason for purchasing software, deficiencies of the current system or method, user and data processing requirements, user and management reporting requirements, system interfaces to other systems, and the in-house resources needed to install and maintain the system.

After the user requirements analysis is completed, the direct and indirect costs of installing and maintaining purchased software should be compared to other business alternatives such as the use of service bureaus, modifications to existing applications, or manual systems. The capabilities and costs of each alternative should be analyzed and compared in a common format (e.g., a spreadsheet). The purchased software alternative should include the costs of modifications to existing data processing systems and expected return on investment.

PURCHASED SOFTWARE EVALUATION GUIDELINES

4.18.4 FACTORS FOR CONSIDERATION

If the results of the user requirements analysis and benefit study indicate purchased software is an effective and preferred solution, the following factors should be evaluated.

- **Financial Stability of the Company** - The statements and resources of the software company should be analyzed to determine if the company is financially sound and has the resources to support and maintain the software package during its estimated life span. This analysis is especially important if the vendor is responsible for future modifications to the software programs. In these cases, procedures should be established to analyze the financial statements, performance, and stability of the company on an annual basis.
- **Contract Review** – The software company's contract should be reviewed by appropriate management, purchasing, and the City Attorney's office to identify potential risks for the city. This review should identify the contract deliverables, schedule delivery dates, method of delivery, documentation, and other key contact elements and terms. It should also include the obligations of the software company to support the software after purchase, furnish updates, and arrange for the program source code and documentation the software company should go out of business. The provisions for terminating or extending the contract should be clearly spelled out. Recourse for monetary losses as a direct result of errors in the software should also be considered. Requirements for annual financial information, preferably audited, should be incorporated into the contract. If the investment is substantial, the contract should include the the right of internal audit staff to perform examinations of software companies for risk and control issues relating to software purchases
  - o Jurisdiction - attempt to have the vendor agree that the contract be interpreted and enforced pursuant to the laws of the State of Nevada.
  - o Arbitration - attempt to have the vendor agree to binding arbitration, if disputes arise, according to the rules of the American Arbitration Association as established and practiced in Las Vegas, Nevada.

PURCHASED SOFTWARE EVALUATION GUIDELINES

- **User References** - References are an important source of information in evaluating vendor packages. A user reference list of other installations using the software package should be obtained from the vendor. These companies should be contacted to obtain information such as the software package purchased, the computer system used to run the software, modifications that were made after installation, the length of time in use, the quality of the vendor conversion support, performance on similar hardware, and other pertinent information. Onsite visits to other installations that have installed the software on a similar computer system should be considered before making a substantial investment in a software package. Care should also be taken in purchasing software that has not been installed and thoroughly tested in other locations.
- **Audit and Security Considerations** – Software packages should be reviewed for security controls and audit trails such as access to data files, authorizations, password controls, data access logs, reporting of file maintenance, reporting of security violations, and capabilities of utility programs to alter data.
- **Life Span of the Product** – The age of the software, the number of updates issued since it was developed, the software vendor's plans for future modifications, and the useful life of the package should be evaluated against the city's short and long term strategic plans.
- **Documentation** - The documentation and manuals provided with the software package, and on-line help programs, if the system is interactive, should be carefully reviewed by Information Technologies and the appropriate User Departments for content, readability, and completeness. This review should include input and output reports, compliance with in-house standards, and documentation provided with modifications.
- **Testing** – Vendors should test all parts of the system in a systematic manner. Information on the testing procedures performed by the vendor should be obtained and evaluated. This information should include test plans, the hardware used for testing, and the method used to verify that the software calculations meet statutory requirements.
- **Conversion Assistance** – The background and experience level of software company personnel assisting the city in conversion planning, support, and training activities should be obtained and evaluated. The vendor should provide a detailed schedule of pre and post conversion support activities with associated costs. Conversion support materials should be carefully reviewed for quality, readability and completeness. The software company internal resources required to support conversion training should also be evaluated. The quality of conversion support provided by the vendor should be verified when checking user references.

PURCHASED SOFTWARE EVALUATION GUIDELINES

- **Maintenance Support** – The capability of the vendor company to provide timely, on-going maintenance support for user programming requests, product updates, version continuity and statutory changes should be evaluated. The content, frequency and costs of previously-issued software updates should be reviewed. The software should also be evaluated for report-writing capabilities that permit inhouse personnel to produce new or specialized reports for management, user departments, or to comply with regulatory requirements. If vendor programming is required for report modifications, these costs should be considered in the evaluation.
- **Software Installation** – After evaluation and selection of a software package that meets the needs of the city, the software contract should be approved by city management, appropriate user groups, Information Technologies, and City Council. Management should provide for an effective project control system to facilitate planning and implementation of the software. Liaison personnel should also be designated to manage the vendor relationship and coordinate the software installation**.**

4.18.5 PURCHASED SOFTWARE EVALUATION GUIDELINES INTERNAL LINK
Intranet readers may access the document at:

Purchased Software Evaluation Guidelines

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.19 REPORT REQUEST POLICY

4.19.1 PURPOSE

To set forth the policy for documenting the creation and modification of in-house developed reports.

4.19.2 SCOPE

Information Technologies Employees

4.19.3 OVERVIEW

Because report development can be a complex activity, particularly when intended for implementation in a multi-user environment, programmers are requested to create reports in accordance with business/user requests and requirements. Therefore a more formal report development methodology is required.

The Application Services Division within the Department of Information Technologies utilizes the I.T. Request Form when developing or modifying inhouse-developed reports. The I.T. Request and the ITCCC (IT Configuration Control Committee) Request forms must be presented to the ITCCC (via e-mail) before placing the report into the production environment. Typically, managerial approvals can be obtained for report requests; however, reports still must be documented before introduction into production environments.

Three pieces of documentation are required before a report can be moved into production and used by users in the production environment:

- The completed I.T. Request Form
- The completed ITCCC Request Form
- Sample output (from a test instance) of the report

New or modified reports can only be implemented after Manager, Supervisor or ITCCC approval. Installation and deployment may require assistance from a System Administrator or Client Support.

4.19.4 REPORT REQUEST POLICY INTERNAL LINK

Intranet readers may access the document at:

Report Request Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.20 REPORT REQUEST FORM PROCEDURE

4.20.1 PURPOSE

To establish procedures for use of report request forms.

4.20.2 SCOPE

Information Technologies Employees

4.20.3 OVERVIEW

The goal of documenting report requests is to establish a set of requirements and parameters so that the reports can be quickly recreated and/or modified by someone other than the original programmer. A report is defined as "any scripted or coded extraction of information or data from a database or data file to a screen, file or printer for the purpose of previewing or printing." This includes, but is not limited to, report applications written in VB, Delphi, HTML, ASP, Crystal Reports, Oracle Reports and MS Access. To facilitate the tracking process, two existing change request forms are utilized:

1) Information Technologies Request Form
2) I.T. Configuration Control Committee (ITCCC) Request Form

This document pertains to the Information Technologies Request Form form, which is used by Information Technologies Applications Services Division staff whenever a report is created or modified.

Responsibilities are delineated in this document, and step-by-step procedures for proper submission are given. These procedures include filling out the additional ITCCC Request Form and notification of the ITCCC committee via e-mail.

Typically, reports can receive managerial approval by the ITCCC and do not have to undergo the formal approval process. However, their introduction into the production environment still has to be documented.

4.20.4 REPORT REQUEST FORM PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

Report Request Form Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.21 REPORTING MICROCOMPUTER PROBLEMS

4.21.1 PURPOSE

To describe the process for reporting microcomputer problems.

4.21.2 SCOPE

All employees.

4.21.3 OVERVIEW

The Microcomputer Support Section offers a variety of services to city employees who work with microcomputers. The Department of Information Technologies has established a Help Desk for coordinating support issues concerning computer problems, mainframe terminals requests, and issues related to telephones.

When calling the Help Desk, users of this service are reminded to have their system ID numbers ready when making their calls as well as the name and model number of their computer or printer, and the application that was running when the problem occurred.

If not answered directly, calls are placed into queues and responded to in the order received. If the call is not answered within five minutes, it is forwarded to voice mail.

After the problem report is received, it is entered into a call-logging database, which is prioritized according to a number of factors, including the seriousness and urgency of the problem. The Help Desk does not schedule repair actions directly but reports them to the appropriate action agency. A representative of that agency (Microcomputer Support, Computer Operations, Telecommunications, etc.,) will contact the requestor about the service needs.

Emergencies will usually be responded to within two to four hours. Other calls typically are resolved in 72 hours. Service provided by third-parties usually occurs within 24 to 72 hours.

Microcomputer Support has no system or printer loaners and stores only a few replacement parts such as keyboards, mice, and floppy drives. Nevertheless, the staff will make every effort to provide as fast a resolution as is needed by the circumstances.

REPORTING MICROCOMPUTER PROBLEMS

Users are asked to provide at least two weeks advance notice for equipment moves, new systems, and new wiring as these request require analysis and planning, and may necessitate scheduling through outside firms such as Sprint.

4.21.4 REPORTING COMPUTER PROBLEMS INTERNAL LINK

Intranet readers may access the document at:

Reporting Microcomputer Problems

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.22 SOFTWARE CHANGE CONTROL POLICY

4.22.1 PURPOSE

To set forth the policy regarding changes to systems, database, and applications software.

4.22.2 SCOPE

- Department of Information Technologies (IT)
- Computer Users

4.22.3 OVERVIEW

All software and database updates will be initiated in writing via a Change Request form that establishes a request date, who needs the change and why, plus other appropriate descriptive information. No changes to implemented application software or to PRODUCTION environment (user) data will be made by I.T. staff (except for systems and database administrators) without prior approval from proper authority.

Separate application environments are provided by I.T. to control the status of projects or programs and to preclude the possibility of inadvertent (or deliberate) damage to live data. They are:

- A DEVELOPMENT instance (environment), dedicated to I.T. development and testing
- A TRAINING instance, dedicated to user testing and training
- A TEST instance, dedicated to user testing and training
- A PRODUCTION instance, dedicated to live use

Although these systems will be linked together for data and program transfer purposes, the linkage mechanism is restricted so as to separate the PRODUCTION software and data from routine accessing by I.T. programming staff or any group charged with development and testing. Ideally, only object code versions of application programs reside on the PRODUCTION computers to further protect data from corruption. Exceptions are made under reasonable circumstances, such as to accommodate system operational requirements. All transactions initiated by users that alter PRODUCTION data must occur via form (screen) programs that have been acquired by or developed by IT.

SOFTWARE CHANGE CONTROL POLICY

The responsibilities for carrying out software-related changes are as follows:

- Systems Administration Specialists, or designated backups, perform all changes to systems operating software (whether based on servers or client computers).
- Database Administrator, System Administration Specialists, or designated backups, make all changes to database software and database structures.
- Applications Services Division systems analysts, programmers, or designated backups carry out all changes to applications software.

An I.T. Configuration Control Committee is responsible for overseeing and controlling all processes related to the modification of systems software, applications software (both inhouse-developed and purchased), data structures, and data. This committee considers all significant requests for system changes and examines not only how they might affect the software or database being modified but other systems as well. The membership is described in the Software Development Life Cycle Policy and the ITCCC Charter.

A Master Library of project or program versions, to which I.T. staff has restricted access, is maintained within a secure environment. This library consists of the latest implemented copy as well as the two previously-implemented copies of all inhouse-developed source code. For purchased systems, object code is maintained in the library providing that the vendor licensing agreement does not preclude it. Source code can be checked out of the libraries for maintenance or recovery purposes.

In addition to Master Library copies, backups on appropriate permanent media are made and maintained for all new object code versions (and the accompanying source, if applicable) of software being placed into PRODUCTION. Copies of backups are routinely transferred off site to provide for contingency software recovery. For purchased applications software, I.T. requires that manufacturers provide, as part of the contract, a copy of the latest source code version in escrow at a secure and offsite third-party location to which I.T. has the name, address, and phone number.

A Version Control System is utilized to track key information associated with current implemented systems as well as previous ones. This consists of items such as project or program names, version numbers, responsible person, information describing the changes, dates changed, etc. See Version Control Policy.

SOFTWARE CHANGE CONTROL POLICY

All screen forms and other application programs must be carefully tested by I.T. and the affected users to ensure that necessary security functions are present and that the program functions are error-free. No program testing is allowed to take place on the PRODUCTION computers with the exception of load and performance testing under carefully-controlled conditions.

All related documentation, such as client operation guides, data dictionaries, help checklists, etc., must be updated before a system change can be implemented. In emergency situations, the Director of Information Technologies can waive this requirement in order to return software to operational status quickly, with the documentation updating to occur as quickly as possible after change implementation.

All changes must be logged so that previous modifications can be quickly located and confidently identified. Once changes to a system have been completed and tested or new versions from a supplier tested, the modifications may be implemented only after proper authorization has been secured. Significant changes must be approved by a responsible person outside of the Division performing the modification before implementation. Periodic self-assessments are conducted to ensure that this process is being followed.

4.22.4 SOFTWARE CHANGE CONTROL POLICY INTERNAL LINK

Intranet readers may access the document at:

Software Change Control Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.23 SOFTWARE DEVELOPMENT LIFE CYCLE POLICY

4.23.1 PURPOSE

To set forth the policy for utilizing a Software Development Life Cycle approach when developing or purchasing new software systems.

4.23.2 SCOPE

Department of Information Technologies (I.T.) Staff

4.23.3 OVERVIEW

Because software development is such a complex and error-prone activity, particularly when intended for implementation in a multi-user environment, a formal methodology is needed to reduce errors. The Department of Information Technologies utilizes a Software Development Life Cycle (SDLC) project management approach when developing or purchasing new applications software. An SDLC tracks a software project's important stages from planning through development and finally to implementation, helping to ensure that developers have considered each aspect carefully.

The significant stages in the life cycle of a software development project are:

- Planning
- Requirements Definition
- Functional Design
- System Design
- Programming
- Integration and Testing
- Installation and Acceptance
- Maintenance (on-going)

SOFTWARE DEVELOPMENT LIFE CYCLE POLICY

The detailed instructions for carrying out the SDLC's considerable task are described in a separate document entitled Software Engineering Methodology (SEM) Procedure. This type of project management tool reduces errors in the delivered product to a minimum and, because of the emphasis on proper planning and communication, insures that the client is getting a product that performs as specified. I.T. has adapted the SEM originally developed by the U.S. Department of Energy (D.O.E.) in 1996 for SDLC purposes due to its low cost (acquired free from the Internet), comprehensiveness (400+ pages) and time to implementation (immediate vs. 12 months of inhouse development by a team).

A Version Control System as described in the Version Control Policy shall be utilized both during development and after implementation of all new software systems. The Version Control system will meet necessary security requirements limiting the updating and access of software to authorized persons only.

4.23.4 MASTER LIBRARY UTILIZATION AND BACKUPS

A Master Library in the TEST environment of project or program versions, to which I.T. staff shall have restricted access, will be maintained within a secure environment. This library will consist of, at a minimum, the latest implemented copy as well as the two previously-implemented copies of all inhouse-developed source code. For purchased systems, object code will be maintained in the library providing that the vendor licensing agreement does not preclude it. Source code will be checked out of the libraries for maintenance or recovery purposes. A Systems Administrator will be designated to maintain the Master Library utilizing the Version Control System.

In addition to library copies, backups on appropriate permanent media will be made and maintained for all new object code versions (and the accompanying source, if applicable) of software being placed into the PRODUCTION environment.

SOFTWARE DEVELOPMENT LIFE CYCLE POLICY

4.23.5 PROJECT OVERSIGHT

Depending upon the project scope, an I.T.-guided Project Control Committee (not the Configuration Control Committee) will oversee and control all processes related to the design, development, testing, and implementation of new software (both applications and database), whether inhouse-developed or purchased. This committee will consist of I.T. project team members and prospective users of the software and/or associated hardware from client departments. In the case of enterprise-wide systems, this guidance will be provided by the City Managers Office. Meetings will be held as often as deemed necessary by the joint group members (usually weekly at a minimum). New programs designed to complement existing systems will be overseen and coordinated through the I.T. project team. Client involvement in all project phases will occur as appropriate.

4.23.6 CLIENT UPDATES TO DATABASES

All transactions initiated by clients that alter production data will occur via forms (screens) that have been acquired or developed by I.T. These forms will be carefully tested by I.T. and the affected clients to ensure that necessary security functions are present in all cases and that program functions are error-free.

4.23.7 SYSTEM AND DATABASE UPDATES

- All manipulation of Server operating software will be made by the Systems Administration Specialists responsible for each of the operating systems or their designated backups.
- All manipulation of Client-resident software for development, testing, and implementation will be made with the coordination of the Support Division.
- All manipulation of database structures will be made by the assigned Database Administrator, Systems Administration Specialists, or designated backup personnel.

4.23.8 SOFTWARE CONTRACTS

All software development contracts are written to require the contractor to either use the adopted SEM for SDLC purposes or to have their SDLC methodology approved by the I.T. Configuration Control Committee or City Managers Office prior to their accomplishing any development work for the city.

SOFTWARE DEVELOPMENT LIFE CYCLE POLICY

4.23.9 RESPONSIBILITIES

SDLC utilization involves I.T. staff members as follows:

- The Projects Division Manager: responsible for team leads for all IT-related projects and for quality assurance
- The Development Division Manager: responsible for application, database, and operating system changes through a staff of systems analysts, system administrators, and programmers
- The Systems Division Manager: attends to all aspects of computer operations and assists the Version Control process with Master Library backups and maintenance of the Version Control software through a staff of systems administrators and computer operators
- The Support Division Manager: responsible for the Support Desk
- The Quality Assurance Administrator: responsible for defining Change Control and Version Control procedures for software and database maintenance and for assuring that these practices are followed
- The Information Security and Contingency Administrator: ensures that all aspects involving data and program security are considered and followed when making system changes and when utilizing a Version Control System
- System Administrators: responsible for maintaining Master Libraries of projects, programs, and related documentation and for checking versions in and out of the Master Library, utilizing the Version Control System
- Systems Analysts and Programmers: responsible for creating applications software and interfaces to purchased software
- Configuration Control Committee: responsible for overseeing and controlling all processes related to the modification of systems software, applications software (both inhouse-developed and purchased), data structures, and data. This committee considers all significant requests for system changes and examines not only how they might affect the software or database being modified but other systems as well. The membership consists of the I.T. Division Managers, Quality Assurance Administrator, Information Security and Contingency Administrator, and a member of the City Auditor's Office. The Director of I.T. and a member of the City Managers Office may attend as appropriate.

4.23.10 SOFTWARE DEVELOPMENT LIFE CYCLE POLICY INTERNAL LINK

Intranet readers may access the document at:

Software Development Life Cycle Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.24 SOFTWARE TESTING POLICY

4.24.1 PURPOSE

To establish a policy to encourage, promote and ensure computer software is thoroughly tested so that defects and problems can be identified and fixed and software requirements can be validated.

4.24.2 SCOPE

Department of Information Technologies employees and non-IT city staff assigned as team members to projects managed by I.T.

4.24.3 OVERVIEW

Software testing is being enforced to enhance the quality of inhouse-developed and purchased software. Testing is an important part of both the software development and software selection processes. There are a variety of tests that should be performed on any new product introduced into the production computing environment. When properly performed and measured against a set of expected results, these tests help to minimize conflicts with existing software and hardware and allow us to build or invest in high quality, secure, and reliable software.

Whether the software is COTS (Commercial Off-The-Shelf) or inhouse developed, a new release, an upgrade, an update, a patch or a service pack, all software must have some level of testing performed and documented on it prior to deployment and introduction into the production computing environment. These tests have to be conducted in accordance with the appropriate software testing procedures.

Exceptions or waivers to this policy can only be granted by the Director of Information Technologies (at any time) or the Security Administrator or managers (during an emergency event).

A test plan must be prepared and finalized with each software package in accordance with Quality Assurance group standards and procedures. Depending upon the scope of testing, Quality Assurance personnel oversee all processes related to the testing whether inhouse developed or purchased. The testing process requires the input of the I.T. staff and prospective users of the software and/or associated hardware. Meetings are held to review the test scripts and results of testing with the I.T. staff and prospective users.

SOFTWARE TESTING POLICY

4.24.4 SOFTWARE TESTING TYPES

The software testing types used by I.T., along with their definitions, are listed below.

- Usability testing – measure how well people can actually use something (such as a web page, a computer interface, a document, or a device) for its intended purpose. If users, or test subjects, have difficulty understanding instructions, manipulating parts, or interpreting feedback, then the developers must go back to the drawing board, improve the design, and test it again. This is better done early in a project, before substantial development effort.
- Data integrity testing – verify that the data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
- Unit testing - isolate each part of the program and showing that the individual parts are testing correctly after a change was introduced.
- Regression testing - re-run previously-executed tests and check whether previously-fixed faults have reemerged
- Integration testing – combine all the parts of an application to determine if they function together correctly. It is usually performed after unit and functional testing. This type of testing is especially relevant to client/server and distributed systems
- System testing – test the combination of applications used in a business process together
- Compatibility testing – test a product's capability to interface with other software and hardware.
- Stress testing – combine an availability test and throughput test. Availability testing involves testing the reliability of the network, database processor, memory, etc. This involves testing the capability to have the support for critical data required by the applications to be up and running in minimum standard conditions. All the architectural components that need to be available are also ensured to be present and functional. Throughput testing is used to test the load-bearing capacity of the system and to measure the response time and throughput of the various components of the system.
- Acceptance testing – have the user test the system and, based on the results, either grant or refuse acceptance of the software/system being tested.
- Sanity test scripts – also referred to as a "smoke test" is a brief run-through of the main functionality of a computer program or other product. It gives a measure of confidence that the system works as expected prior to a more exhaustive round of testing. The sanity test scripts will be executed during a future compatibility test but are written during implementation of the software. The sanity test scripts will contain the minimum function needed to prove the application is still working.

SOFTWARE TESTING POLICY

- Installation testing - Installation testing can be defined as a test install of software onto a copy of the production environment. This test confirms that the application can be installed without expected or unexpected events causing a loss of data or functionality of other systems components.

4.24.5 SOFTWARE TESTING POLICY INTERNAL LINK

Intranet readers may access the document at:

Software Testing Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.25 SOFTWARE TESTING PROCEDURE

4.25.1 PURPOSE

To set forth the procedures that must be followed by Information Technologies and user department personnel for testing software.

4.25.2 SCOPE

This procedure is relative to all the staff in the Department of Information Technologies or user departments called upon to test software.

4.25.3 OVERVIEW

The I.T. Project Coordinator and/or Supervisor creates a Software Testing Plan which is located in the body of templates. The Software Testing Plan and project requirements are reviewed by the Quality Assurance group before coding begins.

Below is a list of types of tests and the staff person(s) responsible.

Test Type	Responsible Staff Person
Usability testing	I.T. Project Coordinator, Developer, Quality Assurance Coordinator
Data Integrity testing	I.T. Project Coordinator, Developer, Database Administrator
Unit testing	Developer
Regression testing	Quality Assurance Coordinator
Integration testing	Quality Assurance Coordinator
System testing	Quality Assurance Coordinator
Compatibility testing	Client Support, I.T. Systems Administrator
Stress testing	Quality Assurance Coordinator
Acceptance testing	User
Sanity testing	Quality Assurance Coordinator
Installation testing	Client Support, I.T. Systems Administrator

Testing types are defined in the Software Testing Policy.

The Quality Assurance Coordinator is responsible for maintaining the automated tests and manual test scripts used in the regression test.

SOFTWARE TESTING PROCEDURE

The Quality Assurance Coordinator and individuals involved with testing must be familiar with the automated tools used by the city for this purpose. As of February, 2005, Mercury Interactive products provide this capability. Mercury Interactive is the repository for all the software requirements, test cases, test plans, testing scripts, defect lists from testing, and automated tests.

- The tester provides three deliverables to the project team: the finished testing plan, the completed test cases, and the defect report.
- The project lead is responsible for entering the requirements into the Mercury Test Director tool.
- The test cases are created by both the project lead and the tester.
- The test plan is started by the project lead and completed by the tester.
- The defect report is maintained by both the tester and the project lead.

There are primarily two types of software, Commercial Off-The-Shelf (COTS) and inhouse developed.

4.25.4 COMMERCIAL OFF-THE-SHELF SOFTWARE (COTS)

Most of the COTS packages are managed by an I.T. Project Coordinator. The various software testing tasks are also overseen by the I.T. Project Coordinator. The job of the tester is to provide input to the project timeline and project deliverables. The following steps must be followed to generate the required deliverables:

1) Identify the degree of testing that will be required by the project (which tests).
2) Identify the test requirements.
3) Formulate an initial estimate of time needed to properly perform testing.
4) Identify resources.
5) Compile the test plan.
6) Verify the test plan with the I.T. Project Coordinator and/or Supervisor.
7) Develop the test cases.
8) Develop the automated test scripts when possible.
9) Perform testing.
10) Provide the I.T. Project Coordinator and/or Supervisor with the defect report.

SOFTWARE TESTING PROCEDURE

4.25.5 INHOUSE-DEVELOPED SOFTWARE

Most of the inhouse development is managed by the Development Supervisor. The various software testing tasks are managed by the Development staff. The following steps must be followed to generate the deliverables:

1) Identify the scope of the testing effort for the project or task.
2) Formulate an initial time estimate.
3) Identify resources.
4) Compile the test plan (minimum of two test types).
5) Verify the test plan with the Supervisor.
6) Develop the test cases.
7) Develop the automated test scripts when possible.
8) Perform testing.
9) Provide the I.T. Project Coordinator and/or Supervisor with the defect report.

SOFTWARE TESTING PROCEDURE

4.25.6 SOFTWARE TESTING LIFE CYCLE

Software testing in conjunction with the project life cycle is defined as follows.

Software Test Type	Project Phase / Activity
Usability testing	Design Phase – usability by the user should be verified before the design phase has been completed and coding begins.
Data Integrity testing	Execution Phase – verification of data needs to be completed before any user or QA testing begins.
Unit testing	Execution Phase – each should be tested as coding is being completed.
Regression testing	Execution Phase – the regression testing can be done any time after the integration testing.
Integration testing	Execution Phase – the integration test of the application should be done after the data integrity and unit testing. The unit test needs to be defect free. User acceptance testing can be performed at the same time.
System testing	Execution Phase – the complete business system test needs to be performed after all the integration testing is completed and defect free.
Compatibility testing	Execution Phase – the complete business system test needs to be performed after all the integration testing is completed and defect free.
Stress testing	Execution Phase – the stress test can be performed any time after the integration testing since it may only be performed on one application of the business process
Acceptance testing	Execution Phase – the user's involvement throughout the project will lend itself to continually testing the applications and system; however, the user must make a decision as to whether the new application is accepted.
Sanity testing	This abbreviated test (open, check basic functions, etc.) is performed in the test environment for quick-checking compatibility after future environmental changes are introduced. (see below).
Installation testing	Execution Phase – should be one of the last tests to be performed during the execution phase and can be performed with the compatibility or integration test.

During the post-implementation phase (45-day support), the sanity test should be created for future compatibility testing after environmental changes are made. The test script in the Mercury Interactive tools must be checked to make sure it can be used for the next regression test, if appropriate.

SOFTWARE TESTING PROCEDURE

4.25.7 SOFTWARE TESTING ENVIRONMENTS

The environment that is appropriate for each of the test types is defined as follows:

Software Test Type	Environment
Usability testing	N/A – the usability test can be performed in a paper format, but screen mockups are more reliable to gather more reliable user opinion.
Data Integrity testing	Development environment or QA Test environment (a test machine that is a copy of production environment)
Unit testing	Development Environment
Regression testing	Test environment
Integration testing	Test environment – several different operating systems may need to be tested
System testing	Test environment
Compatibility testing	Test environment – several different operating systems may need to be tested
Stress testing	Use VMWare and Mercury Interactive tools to simulate production environment
Acceptance testing	Test environment
Sanity testing	Production environment
Installation testing	Test environment – several different operating systems may need to be tested

4.25.8 SOFTWARE TESTING PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

Software Testing Procedure

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.26 SOURCE CODE MANAGEMENT POLICY

4.26.1 PURPOSE

To set forth standards for management of computer language source code in the Information Technologies (I.T.) working environment.

4.26.2 SCOPE

I.T. Employees

4.26.3 OVERVIEW

I.T. utilizes a version control system (PVCS) with all source code developed inhouse as well as forms and reports developed inhouse wherever technically feasible. This allows not only the current (running) version to be identified but also provides for earlier versions to be confidently selected and restored if necessary.

Most inhouse-managed source code is PC-based and is readily adaptable to the PC-based version control system being used. The major software languages covered include:

- Avenue (GIS Applications)
- Visual Basic
- Delphi
- HTML (HyperText Markup Language)
- JavaScript
- ASP (Active Server Pages)

Other PC-based source languages that may come into use in the future willl become subject to this policy.

COBOL source code and Oracle Applications objects (forms, reports, etc.) are not PC-based and must be treated separately. Until an automated system is in place for tracking these programs, I.T. staff members working with non-PC-based source code and objects are responsible for accurate tracking of current running versions and the last two previous versions in accordance with the Version Control Policy. No exception to the above requirement can be made without the approval of the Director of Information Technologies or an I.T. Manager.

SOURCE CODE MANAGEMENT POLICY

Any separate, designated grouping of one or more inhouse-developed source code statements that is compiled or interpreted to run in a Production environment is covered by this policy. This extends from the smallest routine or module called by other programs to the largest program.

Only Team Leads can create project folders within PVCS.

Source code must be placed into the appropriate Technology Repository in PVCS.
- Only by Team Leads
- Before the associated application object code is put into a Production environment

Technology Repositories exist for:
- GIS (Geographic Information Systems)
- Client/Server
- Web
- PL/SQL (Standard Query Language)
- Oracle Scripts

It is not necessary to place source code still under development into PVCS.

4.26.4 SOURCE CODE MANAGEMENT POLICY INTERNAL LINK

Intranet readers may access the document at:

Source Code Management Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.27 USER ACCOUNT TERMINATION PROCEDURE

4.27.1 PURPOSE

To establish a procedure covering the actions taken when a request is received to remove a user from the City of Las Vegas computing environment.

4.27.2 SCOPE

Designated I.T. Personnel and Departmental I.T. Liaisons

4.27.3 OVERVIEW

This procedure is intended to protect city computer resources and supports the principles of the Information Security Policy. This procedure also applies to non-city personnel having access to city computer systems and applications.
An authorized department representative sends an e-mail request to the Director of I.T. or to the Help Desk requesting removal of an employee's or a non-city user's access to the city computing infrastructure. The following steps outline the process for removing a user from the City of Las Vegas computing environment.

1. The Director of I.T. or the Help Desk, (the recipient of the request) informs the ISCA.
2. The Information Security and Contingency Administrator:
   a. Validates the request as authentic and informs the I.T. Systems Administration Specialist of the request.
   b. Contacts the requesting organization while the accounts are being deactivated to obtain direction for the final disposition of any files and e-mails related to the specified user accounts.
3. The I.T. Systems Administration Specialist:
   a. Deactivates all accounts on all systems for the specified user. The accounts are left intact but are restricted from access by the specified user.
   b. Consults with the ISCA on the disposition of the specified user accounts, files, and e-mails.

Note: Under no circumstances are the accounts to be deleted without written request from the requesting department.

USER ACCOUNT TERMINATION PROCEDURE

4.27.4 USER ACCOUNT TERMINATION PROCEDURE INTERNAL LINK

Intranet readers may access the document at:

User Account Termination Procedure (Interim)

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.28 VERSION CONTROL POLICY

4.28.1 PURPOSE

To set forth the policy for establishing and maintaining a Version Control System for managing revisions of the same software in an archive.

4.28.2 SCOPE

Department of Information Technologies (I.T.)
Applies to both source and object code, except in the case of a vendor policy that precludes source ownership

4.28.3 OVERVIEW

The files can consist of source or object code for projects or programs, documentation files, operation schedules, or any project-related material. The archive file contains information about each file revision, allowing the retrieval of current or past versions in a safe and consistent manner. This minimizes the risk of one developer overwriting the files of another, or of a developer making changes to an incorrect version.

4.28.4 VERSION CONTROL SYSTEM SOFTWARE

A Version Control Software System has been established to deal with version control elements. The Version Control software allows "labels" to be attached to specific versions that will associate vendor-supplied version numbers with the ones used internally by the system. There may be different version control systems and libraries to accommodate particular language text editors that cannot encompass the chosen standard. The system meets necessary security requirements limiting the updating and access of software to authorized persons only.

4.28.5 MASTER LIBRARY

An archive, or Master Library, has been established in each of the TEST environments (Development, G.I.S., E.D.M., Intranet, and enterprise projects) to contain current and previous versions of software and related documentation. A Team Lead will be designated in each of the service areas (Development, G.I.S., E.D.M., Intranet, and each enterprise project) to maintain the respective Master Library utilizing the Version Control System.

VERSION CONTROL POLICY

4.28.6 SYSTEM SCOPE

The Version Control System pertains to all application-related software, whether:

- client or server based
- source or object code
- inhouse-developed or purchased

An exception would be purchased software in which a licensing agreement would preclude multiple copies or conflict in some other way. Also, source code copies of purchased software may not be issued by a vendor as part of the original contract.

4.27.7 SOFTWARE CHECK-IN AND CHECK-OUT

Initial versions of software are "checked in" to the Master Library by the Team Lead and given a unique version number. Check-in of previously-identified software also occurs when necessary maintenance has been completed.

When software maintenance is necessary, systems analysts and programmers check out the latest version from the Master Library. Versions of projects, programs, or documentation normally are checked out of the Master Library with a "lock" to prevent those files from being checked out to someone else at the same time.

VERSION CONTROL POLICY

4.28.8 RESPONSIBILITIES

The Version Control System involves the following I.T. staff members:

- The Projects Division Manager: responsible for providing project management and quality assurance staff for I.T. projects
- The Development Division Manager: responsible for application, database, and operating system changes through a staff of systems analysts, system administrators, and programmers. Also checks updated versions of source code back into the Version Control System database in the absence of a Team Lead.
- The Systems Division Manager: attends to all aspects of computer operations and assists the Version Control process with Master Library backups and maintenance of the Version Control software through a staff of systems administrators and computer operators
- The Support Division Manager: responsible for the I.T. Support Desk, communications, and graphic arts operations
- The Quality Assurance Administrator: responsible for defining Change Control and Version Control procedures for software and database maintenance and for assuring that these practices are followed
- The Information Security and Contingency Administrator: ensures that data and program security are considered and followed when making system changes and when utilizing a Version Control System
- Team Leads: responsible for maintaining Master Libraries of projects, programs, and related documentation and for checking versions into the Master Library, utilizing the Version Control System
- Systems Analysts and Programmers: responsible for checking the latest applications source code out of the Version Control System and presenting the updated version to their Team Lead or Division Manager so that it can be placed back into the Version Control System database

4.28.9 VERSION CONTROL POLICY INTERNAL LINK

Intranet readers may access the document at:

Version Control Policy

I.T. GOVERNANCE-RELATED POLICIES/PROCEDURES

4.29 WEB SITE PRIVACY POLICY

4.29.1 PURPOSE

To set forth the policy for issues regarding the privacy of information collected from citizens via the Internet.

4.29.2 SCOPE

All employees. Outside consultants and contractors must be subject to the same information security requirements and have the same information security responsibilities as employees.

4.29.3 OVERVIEW

The City of Las Vegas, its employees, and outside consultants and contractors are obligated to respect, and in many cases, to protect confidential information. There are, however, technical and legal limitations to our ability to protect confidentiality. Each major type of information must have a designated owner and designated custodian. Information owners must establish procedures for sensitive and critical information assets. Information custodians are required to follow the established procedures to properly protect sensitive and critical information.

No one may access confidential records unless specifically authorized to do so, and confidential records must only be used for authorized purposes.

4.29.4 WEB SITE SERVICES

The city provides an Internet web site to inform citizens, to provide interactive opportunities, and to process payments. During interactive response and payment processing, the city may collect certain information which citizens consider personal. This data is necessary to provide the information or services they are seeking and is the same information they would provide when visiting a government office in person. The information collected is subject to the same controls and uses outlined in the access and confidentiality provisions of the City of Las Vegas, State of Nevada, and Federal laws. The city maintains a Privacy Statement on its website containing elements of this privacy policy.

WEB SITE PRIVACY POLICY

4.29.5 NEVADA PUBLIC RECORDS LAW

Nevada Revised Statute (NRS) 239.010 states that, "All public books and public records of a governmental entity, the contents of which are not otherwise declared by law to be confidential, must be open at all times during office hours to inspection by any person…" 'Public records' are regarded as those records which we generate or receive and then maintain in order to conduct city business.

4.29.6 CONFIDENTIAL BY LAW

The City of Las Vegas must protect against disclosure of all information declared by law to be confidential. This includes:

- Personal medical records
- Criminal history records
- Gross revenue data submitted by our business licensees to calculate their business activity tax

Also treated as confidential are credit card numbers and social security numbers used in transactions with the City of Las Vegas.

4.29.7 CRIMINAL PROVISIONS

NRS Chapter 205 provides for criminal prosecution of any employee or city subcontractor who obtains and uses any personal identifying information from city records with the intent to harm another person. Personal identifying information is any information used – alone or in conjunction with other data – to identify a person, such as a name, identifying number, account number, birth date, mother's maiden name, etc. Violation of this statute is a felony, punishable by up to five years in prison. Further, it is no defence that the person who actually uses the information to work the harm is not apprehended or identified.

4.29.8 E-MAIL

E-mail messages sent to any City of Las Vegas address are treated the same as any other written communication. E-mail or other information requests sent to city web sites may be maintained in order to:

- Respond to the request
- Forward the request to the appropriate agency
- Communicate updates to the page that may be of interest to you
- Provide city web designers with valuable customer feedback to assist in improving the website

WEB SITE PRIVACY POLICY

E-mail addresses obtained as a result of a request to a city website are considered public record and, if requested, may be made available to a private company for compensation equal to the cost of providing the information. However, the city does not offer for sale, or solicit buyers for, e-mail addresses.

4.29.9 LINKS TO OTHER WEBSITES

Various commercial Websites may be linked through the city's website. Visitors to those sites may wish to check the privacy statements of these external websites before providing personal information to them.

4.29.10 WEB PRIVACY POLICY INTERNAL LINK

Intranet readers may access the document at:

Website Privacy Policy

SECTION 5 - APPENDIX

5.1 I.T. CONFIGURATION CONTROL COMMITTEE CHARTER
5.2 ORACLE APPLICATION CHANGE CONTROL PROCESS
5.3 ITCCC REQUEST FORM
5.4 IT REQUEST FORM
5.5 SAMPLE BUDGET PREPARATION WORKSHEET
5.6 CLV STANDARD PROJECT PROCESS STEPS
5.7 SAMPLE INTERNET HOME PAGE
5.8 SAMPLE INTRANET HOME PAGE
5.9 SAMPLE I.T. CLIENT SUPPORT INTRANET HOME PAGE
5.10 SAMPLE INTERNET GIS APPLICATION WEB PAGE

APPENDIX

5.1 I.T. CONFIGURATION CONTROL COMMITTEE CHARTER

Information Technologies

Configuration Control Committee

CHARTER

September, 2002

I. T. CONFIGURATION CONTROL COMMITTEE CHARTER

INTRODUCTION

The Department of Information Technologies is resolved to protecting the city's complex production computing environment from unintended interruption.

This objective can be achieved by giving careful consideration to new systems being implemented as well as to changes to existing systems. This charter affirms the right to pursue this objective on a continuing basis.

The city's production computer environments provide automation to improve service and efficiency as well as aid accuracy. The associated work environments are heavily impacted by unscheduled computer downtime that can be experienced when system configuration changes occur.

The Information Technologies Configuration Control Committee (ITCCC) has been formed to consider changes to production computer environments before they occur. This group seeks to minimize service interruptions that may be caused by changes and strives to ensure documentation of systems and operational configurations.

TABLE OF CONTENTS

I. Mission, Goals, and Objectives

II. Responsibilities

III. Representation

IV. Meetings

V. Assumptions, Constraints, and Dependencies

VI. References

I. T. CONFIGURATION CONTROL COMMITTEE CHARTER

Chapter I

MISSION, GOALS, AND OBJECTIVES

Article I

Mission

The mission of the Information Technologies Configuration Control Committee is to protect and document changes to the complex computer environments serving the many city departments and offices by managing the change control process during system modifications.

Article 2

Goals

The primary goal of the ITCCC is to manage changes of configuration to production environments.

Having appropriate areas of interest represented at ITCCC meetings will ensure adequate communication between departmental groups. The ITCCC may analyze available downtime and service interruption statistics to look for trends, types, occurrence times, etc. The committee should also endeavor to determine if there are any procedural gaps to close or committee effectiveness problems to correct. This type of analysis will enable the ITCCC to pursue operational goals of:

- Documenting approved production environment changes
- Procedurally eliminating unsanctioned production environment changes
- Allowing production environment changes to proceed with the confidence that practically all potentially damaging aspects have been considered and adequate testing done
- Reducing service interruption to a low and acceptable level.

I. T. CONFIGURATION CONTROL COMMITTEE CHARTER

Article 3

Objectives

The objectives of the ITCCC are to:

- Consider changes to production environments, whether software, hardware, or operational, before they occur.
- Attempt to minimize possible conflicts and potential risks between system components or to ensure that all items are considered.
- Recommend changes, if necessary, to remove potential obstacles or to address omitted items.
- Vote approval, by majority of the voting membership, to go forward with configuration changes and new system implementations, once all conditions for approval have been satisfied.

Chapter II

RESPONSIBILITIES

Article 4

System Considerations

Changes to operating and network systems must be considered carefully, and a decision made as to the level of "granularity" at which these types of changes will be petitioned to the ITCCC before going forward.

Article 5

Support Considerations

Client support can be performed remotely in many cases, and software on client machines can be installed remotely in large volume. The ITCCC must review changes and consider their impact on users and other systems.

I. T. CONFIGURATION CONTROL COMMITTEE CHARTER

Article 6

Project Considerations

The Project Group in I.T. must be aware of all changes being proposed to production environments in order to fulfill its role in the project planning and coordination process.

Article 7

Development Considerations

The Development Group in I.T. must ensure that all potential software changes to production environments are petitioned before the ITCCC and granted approval before being placed into production.

Article 8

Security Considerations

Logical security considerations must always be taken into account in conjunction with changes to production environments. Security threats may necessitate changes to hardware, software, or operating environments that would not have been considered otherwise.

Article 9

User Considerations

Potential changes may affect users and must always be given appropriate attention. Scheduling may need to be considered. Training might be necessary for users to work in the changed environment. Manuals and documentation may require updating.

Article 10

Risk Assessment

Even though proper testing has been performed in a separate test environment, there may still be risks associated with placing a change into production. These potential impacts must be identified by the ITCCC and taken into account when deciding to move forward or to delay system changes.

I. T. CONFIGURATION CONTROL COMMITTEE CHARTER

Article 11

Additional Considerations

The Quality Assurance function is concerned with identifying potential problems at the earliest possible time during a project and seeks to keep them out of production environments to as great a degree as possible.

Regulatory concerns and industry best practices must be taken into account before new systems and changes to the current environments are implemented.

The impact of configuration control changes on business operations must be considered.

Chapter III

REPRESENTATION

Article 12

Member Positions

The member positions of the ITCCC are as follows:

Director of Information Technologies
IT Manager, Development
IT Manager, Policy and Planning
IT Manager, Support
IT Manager, Systems
Project Officer (CMO)
Information Security and Contingency Administrator (IT)
Quality Assurance Administrator (IT)
Senior Information Technology Auditor (AO)
Secretary (IT)
Others as deemed necessary

I. T. CONFIGURATION CONTROL COMMITTEE CHARTER

Article 13

Voting Procedures

The Director of I.T. is a non-voting member that participates in an advisory capacity. All of the other listed committee members with the exception of the Senior Information Technology Auditor and the Secretary have voting rights. All motions for actions at committee meetings will be carried by a majority of the voting membership (not simply a majority of voting members present).

All actions carried by e-mail will be by approval of a majority of the voting membership. Proxy e-mail voting will not be allowed.

Article 14

Chairmanship

The Quality Assurance Administrator will serve as chairperson to guide the meetings and to prepare and distribute an agenda. If the chairperson cannot be present, a backup person will be designated.

Chapter IV

MEETINGS

Article 15

Routine or Sufficiently-Documented Requests

The ITCCC Change Request Procedure, which documents the details to be followed when submitting a request, allows for requests that are routine in nature or that are adequately documented to be approved through consent.

I. T. CONFIGURATION CONTROL COMMITTEE CHARTER

Article 16

Time

Meetings are to be held weekly. Those submitting items for consideration must do so in advance of scheduled meetings in accordance with the ITCCC Change Request Procedure in order to allow committee members time to familiarize themselves with the proposals and associated issues. Dates and times will be established and maintained by ITCCC member vote and published in the companion ITCCC Change Request Procedure document.

Article 17

Place

Meetings will be held in the I.T. Conference Room on the 5th Floor unless otherwise stipulated.

Article 18

Attendance

Members are requested to attend all meetings. If a member cannot be present at a meeting, a backup person from that particular group or area of expertise may be requested to attend by the absentee member. However, this backup attendee will not have voting rights. A quorum of voting members must be present or the meeting shall be rescheduled.

Article 19

Cancellation

If there are no items to consider during the week a cancellation meeting notice will be distributed.

I. T. CONFIGURATION CONTROL COMMITTEE CHARTER

Article 20

Agendas and Minutes

An agenda shall be prepared and distributed before each meeting listing items to be discussed and their presenters so that committee members will have a chance to consider issues in advance. Minutes will be taken at each meeting from which written minutes will be prepared and, unless prohibited by unusual circumstances, distributed prior to the next scheduled meeting date. The minutes will be reviewed and checked for accuracy, grammar, etc. before dissemination. Outstanding issues will be retained in the minutes from week to week until resolved.

Article 21

Special Circumstances

Special circumstances may require unscheduled meetings or votes to be taken via e-mail. The chairperson will convene the unscheduled meetings and/or collect e-mail votes

Chapter V

ASSUMPTIONS, CONSTRAINTS, AND DEPENDENCIES

Article 22

Assumptions

Information furnished to the committee by others is assumed to be accurate and up to date.

I.T. CONFIGURATION CONTROL COMMITTEE CHARTER

Article 23

Constraints

The ITCCC cannot identify all problems leading to service interruption.
The ITCCC may limit the number of items to be considered at a meeting.

ITCCC members do not research problem details unless requested by the committee as a whole. The committee identifies potential problem areas and requests others to perform the necessary detailed analysis.

Article 24

Dependencies

The ITCCC depends on key Systems, Development, and Support Group personnel to prevent changes from proceeding without ITCCC sanction.

The ITCCC depends on the knowledge and cooperation of all identified parties specifically and all I.T. employees in general for its goals to be achieved.

The level of cooperation of users should increase as they better appreciate that there is a link between improved change coordination and lower service interruption.

Chapter VI

REFERENCES

ITCCC Change Request Procedure

APPENDIX

5.2 ORACLE APPLICATIONS CONTROL PROCESS

PURPOSE

To establish consistent steps for submitting and approving Oracle Change Requests for the TRAIN, TEST, and PROD instances.

SCOPE

Pertains to all Oracle Change Review Committee members and appropriate staff from:

- Department of Information Technologies (IT)
- Department of Finance and Business Services (Finance), and
- Department of Human Resources (HR)

RESPONSIBILITIES

Oracle Change Review Committee – Composed of representatives from module areas of the Oracle applications systems. Voting members review and approve or disapprove proposed changes to the TRAIN, TEST, and PROD instances. All voting members must approve of a change before proceeding.

Oracle Change Review Committee Primary Voting Member – Application module coordinators and I.T. staff representative who approve or disapprove of proposed changes.

Oracle Change Review Committee Backup Voting Member – In the absence of employees with primary responsibility, employees designated to perform:

- Oracle Change Review Committee Voting Member duties, or
- Module Coordinator testing duties

Oracle I.T. Team – Composed of I.T. staff members involved with the operation and integration of Oracle applications and the database.

Requestor – Oracle Change Review Committee members or I.T. staff members who submit proposed changes to the Oracle applications systems.

Oracle Change Control Administrator – I.T. staff person who coordinates the change process. This person:

- Receives change requests
- Notifies Oracle Change Review Committee members of change requests
- Records votes from Oracle Change Review Committee members
- Notifies requestors of approval or disapproval, with copies to Oracle Change Review Committee

ORACLE APPLICATIONS CHANGE CONTROL PROCESS

Module Coordinator – Employee in User area responsible for testing specific modules (for example, General Ledger, Purchasing, Payroll) of the Oracle applications systems.

PROCESS

Change Control Process

The change control process includes the following steps.

1. Requestor:
   Send an e-mail to the Oracle Change Control Administrator. The message must:
   a. State that the request is an Add to the TRAIN or the TEST instance; or
      state that the request is a 'Move from the TRAIN to the TEST instance' or a 'Move from the TEST to the PROD instance.'
   b. Describe what is being changed.
   c. Give a schedule including:
      - When the instance will be available for testing
      - The expected testing completion date
      - The expected implementation date into the new instance.

2. Oracle Change Control Administrator:
   a. Review the submission for completeness.
   b. Assign a new sequence number to make the request unique.
   c. Create a folder in the Oracle Change Committee section of Public Folders for Microsoft Outlook. Preface the title with the sequence number.
   d. Send the schedule request via e-mail to the Change Review Committee requesting approval/disapproval.
   e. Copy the Oracle I.T. Team so that staff is aware of what is being proposed.

3. Oracle Change Review Committee members:
   Review the schedule request.

4. Voting members of the Oracle Change Review Committee:
   Send an e-mail to the Oracle Change Control Administrator either:
      - Approving the request, or
      - Disapproving the request, with a reason why

5. Oracle Change Control Administrator:
   a. Advise the Requestor and the Oracle Change Review Committee of any changes to the plan or the schedule.
   b. Advise the Requestor and the Oracle Change Review Committee that the plan has been approved or disapproved (and why). If disapproved, the procedure stops here.

ORACLE APPLICATIONS CHANGE CONTROL PROCESS

6. Requestor:
   Send an e-mail to the Oracle Change Control Administrator requesting approval to move the change to the new instance upon completion of necessary testing.

7. Oracle Change Control Administrator:
   Send an e-mail to the Oracle Change Review Committee requesting approval or disapproval to implement after all testing has been completed successfully. The e-mail request will have the same assigned number with an "a" appended.

8. Module Coordinators:
   a. Perform the testing according to the agreed-upon dates.
   b. Inform your respective voting Change Review Committee member of the test results.

7. Voting members of the Oracle Change Review Committee:
   a. If the original testing deadline will be missed, inform the Oracle Change Review Committee advising the new estimated testing completion time.
   b. Oracle Change Review Committee members:
      Inform the Oracle Change Control Administrator of either:
      - Approval or
      - Disapproval, with a reason why.

8. Oracle Change Control Administrator:
   a. Advise the requestor via e-mail of the approval or disapproval, with a reason why.
   b. Copy the Oracle Change Review Committee and the Oracle I.T. Team.
   c. Make certain that all e-mails have been moved to the appropriate folder.

General Guidelines

Voting members of the Oracle Change Review Committee and Module Coordinators:
Inform your backups when you plan to be absent from work so they can vote in your place.

Voting member backups:
Do not participate in change voting unless the primary voting member is absent.

Generally use e-mail for communication. If you make decisions or process changes over the telephone:
- Document what was discussed with a confirming e-mail message and
- Copy the Oracle Change Control Administrator

ORACLE APPLICATIONS CHANGE CONTROL PROCESS

When to Request Change Control

Follow the Change Control Process outlined above for:

- Patches
- Upgrades *
- System settings
- New module installations *
- Module setup changes
- Oracle standard reports
- First time using of API's
- Backdoor (We do not do this type, but it must be included to make the list complete.)
- Forms
- New formulas
- Changed formulas before being moved to the PROD instance
- New Source API's before being moved to the PROD instance

Testing Level

Conduct full, complete testing for the process types listed above with an asterisk (*). Test critical processes as a minimum for all other types.

When to Send 'Information Only' Requests to Change Control

Send 'Information Only' requests for the following process types. If you are a voting member of the Oracle Change Review Committee, respond only if you have an issue with the request.

- Changing formulas when in TEST, TRAIN, or any instance other than PROD
- Adding elements
- Implementing new CLV reports
- Changing CLV reports
- New Source API's when in TEST, TRAIN, or any instance other than PROD
- Consulting on site
- Permitting dial-in to the system (must be approved by I.T.Systems Infrastructure Management Division first)

When No Change Control is Needed

Do not submit Change Control Requests for:

- Table changes (maintenance to data)
- Rate changes

APPENDIX

5.3 ITCCC REQUEST FORM

Requesting Information			
Date Form Submitted		**Desired Implementation Date**	
Request/Requirement (Move to Prod, Emergency, etc.)			
Type (Hardware, Software, Operational)			

Project and Staff

Requestor			
Requesting Department			
Project Name		**Project Coordinator/Mgr**	
Team Lead/Captain		**HEAT Number**	

Background

Application		**Inhouse/Third Party, etc.**	
Problem Description/ Reason for Change			

Testing Information			
Test Date Start		**Test Date End**	
Change Description			
Testing and/or Supporting Documentation			
Implementation Plan			
•	**Risk to Which System(s) and How?**		
•	**Security Requirements**		
•	**Backup/Rollback/ Restore Process**		
•	**Special Instructions**		

Change Control Information			
ITCCC Meeting Date		**Approve/Disapprove/Cancel**	
Action Date		**By (Committee, E-mail, Manager, etc.)**	
Conditions		**Comments**	

Implementation Information			
Moved to Production Date		**Time**	
By IT Staff Person			
Comments			

APPENDIX

5.4 I.T. REQUEST FORM

City of Las Vegas

Information Technologies Request Form

**1 ▪ Type of Request		
❑ New Employee Setup	❑ Interdepartmental/divisional Move	❑ Equipment Move
❑ Modify Employee Setup	❑ Other *(describe)*_____	
❑ Delete Employee Setup	Date of Request: _____ Date Required: _____	

2 ▪ Employee Info (For transfers, it is useful to include the old and new Dept/Div/Section, address and telephone number)		
**Employee's LEGAL Name *(Last, First, M.I.)*. ↓ Preferred Name↓		**Employee's Social Security Number ↓
**Department Name ↓	** Division Name ↓	Section Name ↓
**Address/Location (*Include Suite #, Floor, etc. Be Descriptive as possible*):		**Phone No.:

3 ▪ Network/Systems Access	
❑ Standard - *Includes Email, Intranet (Tribune) access, Home folder on network F:/ drive*	
❑ Email Lists [Distribution Lists] - *By default, user is only added to All Exchange Users and Department's master list.*	❑ NT Group Membership - *By default, a user is only added to corresponding Dept/Div/Section groups*
❑ Special File Permissions – *Requests for access to folders outside the requesting Department require written authorization from the other Department's Director* ❑ Clone Account – *If another person in the Dept/Div. has the same accesses as this person needs provide the name below.* Individual to Clone – ❑ Internet (Worldwide Web)	❑ Other Network Access Requirements - *(describe)* ❑ RAS (Remote Access Services)(*complete Page 3 of this form and place Charge Org. information in Section 7.)* ❑ Access Restrictions - *list restrictions on the days, hours or systems available to this person.*

4 ▪ Computer Applications/Software - *Some commercial software must be purchased by IT. Please include your Charge Org. and WBS/Activity Code in section 7 for each request.*	
❑ Standard - *Includes Microsoft Word, Excel, Access, and PowerPoint*	
❑ Non-Standard – *Software not purchased separately (i.e., MS Query, Acrobat Reader, specific program executables, Winframe Server Mapping)* _____ _____ Applications *(many applications require training before access)* Oracle Financials ❑ Inquiry ❑ iProcurement Other Responsibility _____ ❑ Hansen ❑ Class ❑ CARS ❑ Other CLV Applications *(describe)*	Commercial Applications ❑ AutoCAD *(Prior training required)* ❑ CTC Bridge ❑ Crystal Reports ❑ Other Commercial Applications *(describe)* GIS Applications *(Prior training required)* ❑ GIS Access ❑ ArcIMS (specify view) ❑ ArcView ❑ ArcInfo ❑ Other GIS Applications *(describe)* Mainframe Applications:

*Mandatory Fields are identified by ***
If these fields are not completed the form will be returned.

Page 1 of 3
Last Revised 12/1/04

I.T. REQUEST FORM (Continued)

City of Las Vegas

Information Technologies Request Form

☐ User will require new Hardware (complete Item 5)		☐ User will use existing hardware	
5 ▪ Hardware Purchases - *Please include your Charge Org. and WBS/Activity Code in section 7 for each request.*			
☐ System 1 – *(17" monitor)*	☐ System 2 – *(20" monitor)*	☐ System 3 – *(Notebook)*	☐ PDA
☐ Laser Printer	☐ Other Printer *(Model):*		☐ Cash Register Receipt Printer
☐ Printer Network Card	☐ Modem *(System 1 or 2)*	☐ Modem *(System 3)*	☐ Scanner *(Model):*
6 ▪ Telephone Equipment & Services - *Please include your Charge Org. and WBS/Activity Code in section 7.*			
☐ Telephone Line	☐ For use with a Modem	☐ Voice Mail	
☐ Telephone – *Describe Model & Features:*		☐ Number to allow receipt of faxes via PC	
☐ Use Existing Number	☐ New Number Required	☐ Long Distance Code	
☐ Cellular Phone	☐ Radio		
**** 7 ▪ Funding Source** (Maintaining Org. must be provided if different than Purchasing Org.)			
Purchasing Org. _____ Acct _____ WBS or W/A# _____ Task _____ Opt _____		Maintaining Org. _____ WBS or W/A# _____ Task _____ Opt	
Grant Org. _____ Acct _____ WBS or W/A# Task _____ Opt _____		*Note: WBS number/Activity Code has to be included along with the organization number.*	
8 ▪ Special Instructions			
Please state any special instructions or requirements:			
**** 9 ▪ Employee Acknowledgment**			
I have read, and agree to abide by, the *Use of IT Resources* document. I understand that violation of this document or other City policies, current or as amended, gives the City of Las Vegas the right to deny access privileges and, if warranted, take further disciplinary action under applicable State and Federal laws.			
Employee Signature:		Date:	
**** 10 ▪ Approvals**			
TUC Coordinator's Initials:		Date:	
Supervisor's Signature:		Date:	
Manager's Signature:		Date:	
Director's Signature:		Date:	
IT Use Only			
HEAT No:			

*Mandatory Fields are identified by ***
If these fields are not completed the form will be returned.

Page 2 of 3
Last Revised 12/1/04

I.T. REQUEST FORM (Continued)

5.5 SAMPLE BUDGET PREPARATION WORKSHEET

INSTRUCTIONS FOR SCHEDULE 2
NEW OR EXPANDED PROGRAM ANALYSIS

OVERVIEW:

In Program Budgeting it is essential to establish indicators that show the effectiveness of the program reaching its goal. By developing mechanisms for collecting and analyzing data and how the program is functioning, and monitoring progress to determine what adjustments or changes need to be made to reach the desired outcome, a more effective delivery of services can be provided to the citizens of Las Vegas.

Better decisions are made when a program's goals and objectives identify which services or outputs are supplied by which resources or inputs. From an operational perspective, program structuring can indicate service delivery problems and encourage the search for more effective and efficient operating methods to meet program objectives. The Department will provide a copy of their Business Plan as documentation supporting base request.

Each Department should develop a clear and concise description of the program(s) for which it is responsible. This should support the strategic plan and department goals and objectives submitted for the Quarterly Progress Report.

Schedule 2 provides you with a format for defining each of your new or expanded programs and establishing quantifiable performance measurements. This information will assist in the continuing implementation of program budgeting.

COMPLETING THE SCHEDULE:

Schedule 2, New or Expanded Program Analysis Questionnaire - one schedule for each new or expanded program within the department; attach to appropriate divisional submission.

List the name of the program, responsible point of contact, and responsible budget organization. If the program is related to a strategic plan item, please list applicable item.

There are four sections included in this schedule:

1. Introductory Information - provides general information and an overview of the program.
2. Program Purpose - identifies desired outcome of the program.
3. Program Fiscal Impacts - assesses the costs associated with the program.
4. Program Monitoring - determines how performance will be monitored and if contingency plans have been made to ensure a successful program.

Answer all sections and questions, if additional space is needed for any of these sections or questions, please attach additional sheets referencing the section and question.

SAMPLE BUDGET PREPARATION WORKSHEET (Continued)

DEPARTMENT BUDGET
SCHEDULE 2
NEW OR EXPANDED PROGRAM ANALYSIS QUESTIONNAIRE

PROGRAM NAME: _____

Who is directly responsible for this program? Title: Name: Org:

Is this program part of a strategic plan item? Item:

	Description	Yes	No	Comments
INTRODUCTORY INFORMATION				
1	Is this a new or expanded program?	☐	☐	
2	Is there a starting date for implementation of the program?	☐	☐	If yes list date:
3	Will this be a continuing program?	☐	☐	List duration:
4	Will this program replace or reduce another program?	☐	☐	If yes list program affected:
5	Will this program reduce cost?	☐	☐	If yes list cost elements reduced:
6	Will this program generate additional revenue?	☐	☐	If yes list source and amount
PROGRAM PURPOSE				
1	Is the request being made to improve quality of work?	☐	☐	If yes list improvements desired:
2	Is the request being made to increase quantity of work?	☐	☐	If yes list increase amount:
3	Is the request associated with a technological change?	☐	☐	If yes list change:

SAMPLE BUDGET PREPARATION WORKSHEET (Continued)

DEPARTMENT BUDGET
SCHEDULE 2
NEW OR EXPANDED PROGRAM ANALYSIS QUESTIONNAIRE
(Continued…)

	Description	Yes	No	Comments
PROGRAM FISCAL IMPACTS				
1	Can existing employees be cross-trained or reallocated?			If yes list employees:
2	Are vacant positions available?	☐	☐	If yes list the number and type of positions:
3	Are additional positions needed?	☐	☐	If yes list the number and type of positions:
4	Is training or certification required?	☐	☐	If yes list type and cost:
5	Are additional services and supplies needed?	☐	☐	If yes list items and amounts:
6	Is additional capital outlay required?	☐	☐	If yes list items and amounts:
7	Are additional facilities or office space needed?	☐	☐	If yes list amount:
8	Are additional computer resources required?	☐	☐	If yes list (hardware, software, programming):
PROGRAM MONITORING				
1	Are objectives of the program quantifiable and measurable?	☐	☐	If yes list performance measures
2	Has a plan been developed to adequately monitor and evaluate the program?	☐	☐	If yes attach plan:
3	Are there alternatives for meeting the objectives?	☐	☐	If yes attach back up plan
4	Is there a private vendor available to provide this service?	☐	☐	If yes list vendors:

APPENDIX

5.6 CLV STANDARD PROJECT PROCESS STEPS

Step	Finished Work	Available Resources	Work to be Completed	Step Overview	Management Guidance
1.0 Selection	• Identification of a project opportunity.	• Meetings • Reviews • Checklists • Tools: Microsoft Word Excel	• Work Request Requirements • Overview Project Proposal Template • Business Case Template • Project Determination Checklist • Project Type Checklist • Project Selection Scorecard Spreadsheet • Project Selection Checklist	• Describe a business need/opportunity that may require a project to be initiated. • Determine if the Work Request warrants a Project Proposal or if it represents non-project work • Select the project type for the proposed project. • Develop a formal project proposal.	• The Project Proposal is a short version of the Project Charter and should include general objectives and high level estimates of expected benefits. • Estimates of effort, costs, and duration may be included but should indicate ranges and a risk assessment. • If possible, the approach to fulfilling the requirements should be briefly described.
1.99 Selection Gate	• Requirements Overview uirements Overview • Project Proposal • Business Case	• Meetings • Reviews • Checklists • Tools: Microsoft Word PowerPoint	• Project Selection Approval Template • Project Selection Presentation Agenda	• Review the project proposal. • Select one: o Approve for initiation o Request additional information and a further review o Reject the project proposal	• Authorized individual or group will review and approve a proposed project • The decision-making process may vary from one business group to another. • The size and type of project may affect the decision-making process.
2.0 Initiating	• Requirements Overview • Project Proposal • Business Case	• Meetings • Templates • Checklists • Organizational Policies • Historical Information • Stakeholder Analysis • Cost/Benefits Analysis • Tools: Microsoft Word	• Project Charter Template • Initiating Process Checklist	• Create the Project Charter using information from: o Requirements Overview o Project Proposal o Business Case o Additional high-level requirements analysis o Additional high-level stakeholder analysis o Additional high-level cost/benefits analysis	• This step may vary depending upon the type of the project and specific procedures within the organization. • The effort and duration for this step depends upon the scope and complexity of the proposed project.

CLV STANDARD PROJECT PROCESS STEPS (Continued)

Step	Finished Work	Available Resources	Work to be Completed	Step Overview	Management Guidance
2.99 Initiating Gate	• Project Selection Scorecard • Project Charter • Initiating Process Checklist.	• Meetings • Reviews • Checklists • Management Judgment • Tools: Microsoft Word PowerPoint	• Charter Approval Document Template • Project Charter Meeting Agenda	• Obtain official approval of the Project Charter that authorizes the project to begin.	• The Charter Approval Document is normally signed by the sponsor of the project. • This signature gives the project manager the authority to carry out the activities in the project charter.
3.0 Planning	• Project Charter	• Meetings • Reviews • Checklists • Project Planning Process • Stakeholder Knowledge • Tools: Microsoft Word Excel Project	• Requirements Document Template • Work Breakdown Structure Template • Work Breakdown Structure (MS Excel) • Project Schedule Template • Project Schedule Template (MS Project) • Work Package Template • Work Package List Template • Project Budget Template • Project Plan Template • Project Plan Checklist • Planning Process Checklist n	• Create a baseline project plan by defining the project's o Requirements o Schedule o Budget	• The plan is used to guide the execution of the project and is a baseline for measurement and control. • Planning is an iterative process and includes negotiation to ensure the results are achievable. • The plan documents risks and assumptions. For complex projects, use of a scheduling tool like MS Project is recommended.
3.99 Planning Gate	• Project Plan • Project Plan Checklist • Planning Process Checklist	• Meetings • Reviews • Checklists • Management Judgment • Tools: Microsoft Word PowerPower	• Project Plan Approval Template • Project Plan Approval Meeting Agenda	• Obtain the official approval for the project plan. • This approval gives the project manager the authority to move to the execution process of the project based upon the project plan.	• Approval may be by: o Sponsor o User group o Project office members • This may vary depending upon the organization's: o Policies o Type of project o Other variables.

CLV STANDARD PROJECT PROCESS STEPS (Continued)

Step	Finished Work	Available Resources	Work to be Completed	Step Overview	Management Guidance
4.0 Executing	• Project Plan	• Meetings • Reviews • Checklists • General Management Skills • Product Knowledge • Tools: Microsoft Word PowerPoint Project	• Kick Off Meeting Checklist • Kick Off Meeting Agenda • Project Team Organization Chart • The Product of the Project Template • Project Status Report Template • Quality Report Template • Project Issues Log Template • Change Request Form Template • Change Request Log Template	• Carry out the project plan by: o coordinating people and other resources required o performing defined activities o ensuring conformance to contracts o capturing performance data	• From a project management perspective, project execution includes: o contracts management o performance reporting o quality management o change control activities that are performed in parallel with the execution of the core project activities.
5.0 Controlling	• Project Status Report • Change Request Log • Project Issues Log • Quality Report	• Meetings • Reviews • Checklists • Performance Analysis • Tools: Microsoft Word Excel PowerPoint	• Project Performance Report Template • Project Transistion Report Template • Controlling Process Checklist • Issues/Changes Request Meeting Agenda • Project Status Report Meeting Agenda • Project Plan Changes Meeting Agenda	• Control changes to the project: o Scope o Budget o Schedule • Keep stakeholders informed	• The controlling process includes: o monitoring and updating the cost baseline o preventing unauthorized changes o communicating authorized changes o updating the project status o verifying that requirements are being met.
5.99 Controlling Gate	• Project Charter • Project Transition Report • The Product of the Project	• Meetings • Reviews • Checklists • Tools: Microsoft Word	• Product Acceptance Document Template	• Handover of the product to the customer and those responsible for product support	o This step involves transitioning of the completed product to the customer and the formal acceptance of the product by the customer.

CLV STANDARD PROJECT PROCESS STEPS (Continued)

Step	Finished Work	Available Resources	Work to be Completed	Step Overview	Management Guidance
6.0 Closing	• Work Request • Quality Report • Project Performance Report • Product Acceptance Document • Project Selection Checklist • Project Selection Scorecard • Kick Off Meeting Checklist • Controlling Process Checklist	• Meetings • Reviews • Checklists • Performance Reporting • Tools Microsoft Word	• Lessons Learned Document Template • Project Archives Report Template • Closing Process Template	• Bring the project to an orderly end by: o Gathering, compiling, and disseminating project information o Formalizing project completion	• Projects terminate when:: o Their objectives have been met, or o They have been cancelled. • Closure is required regardless of the reasons for termination. • Learning from each project and applying lessons learned are critical aspects of the closing process.
6.99 Closing Gate	• Closing Process Checklist • Product Acceptance Document • The Product of the Project • Project Performance Report	• Meetings • Reviews • Checklists • Tools: Microsoft Word	• Closing Approval Document Template • Project Closing Meeting Agenda	• The official approval for the completion of the project	• Sign off by the sponsor and the customer to acknowledge that o the objectives of the project have been satisfied, or o the project has otherwise reached its end.
7.0 Continuous Improvement	• Lessons Learned Document • Additional documentation (input by user)	• Meetings • Reviews • Checklists • Tools: Microsoft Word PowerPoint	• Continuous Improvement Template • Communications Checklist • Continuous Improvement Meeting Agenda	• Incorporate lessons learned into the improvement process of the organization	• The improvement process involves: o analysis of lessons learned and performance trends o corrective action by the process owner to address opportunities for improvement.

APPENDIX

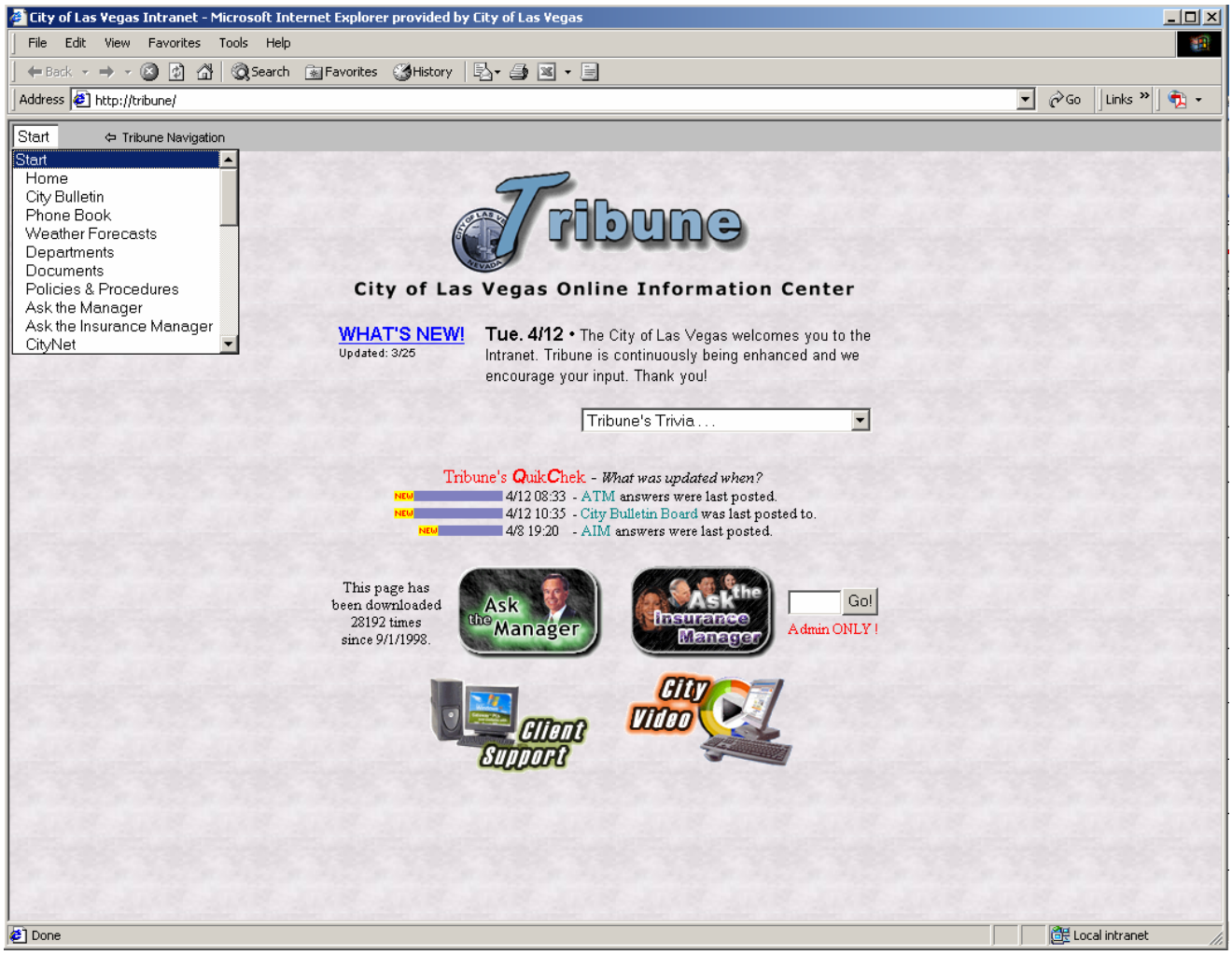
5.7 SAMPLE INTERNET HOME PAGE

Below is a sample of the city's Internet Home Page. The Internet is in the midst of a major revision, seeking to make it less departmentally-focused than n the past.

APPENDIX

5.8 SAMPLE INTRANET HOME PAGE

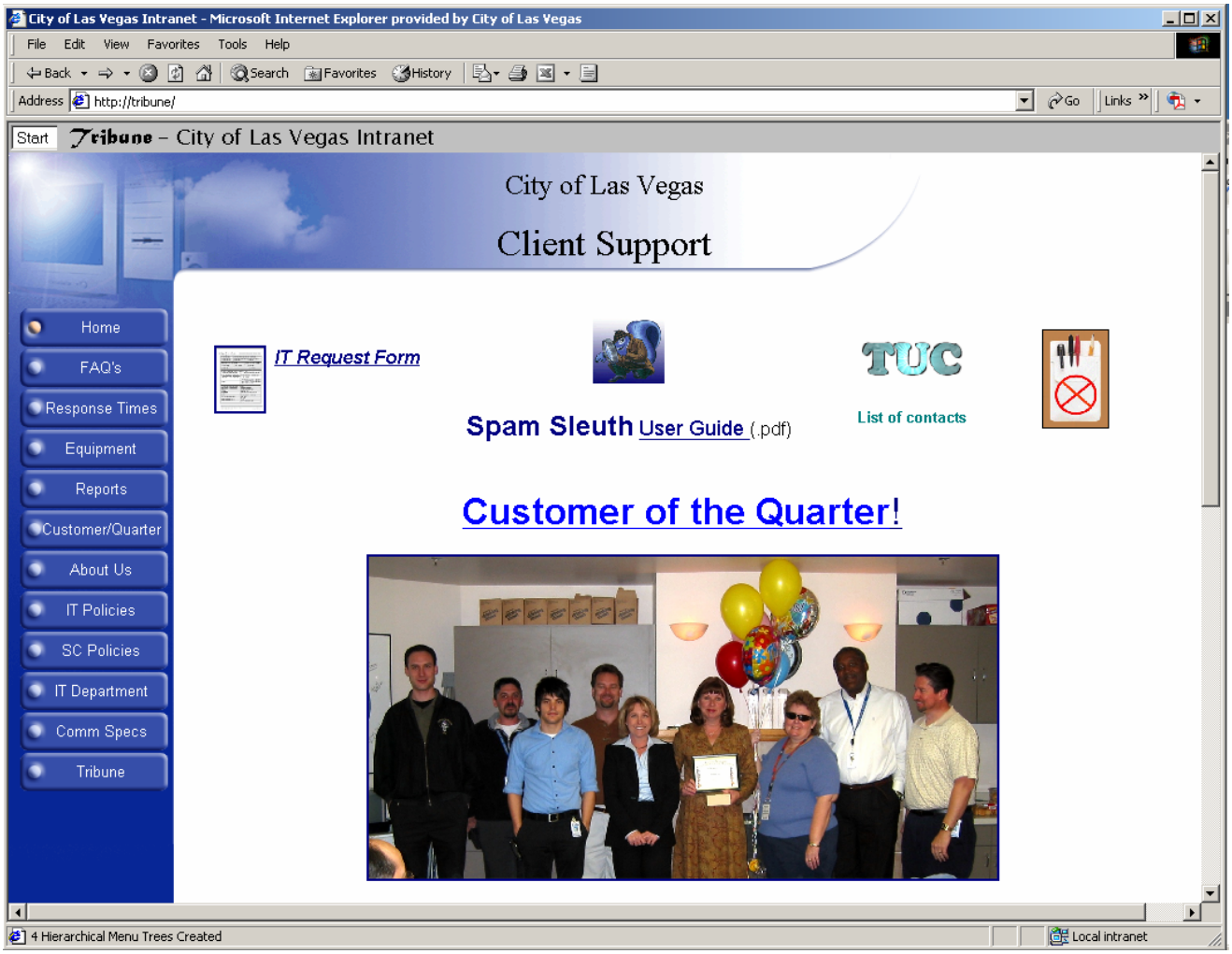
Below is a view of the Home Page for the City's employee-focused Intranet.



APPENDIX

5.9 SAMPLE CLIENT SUPPORT INTRANET HOME PAGE

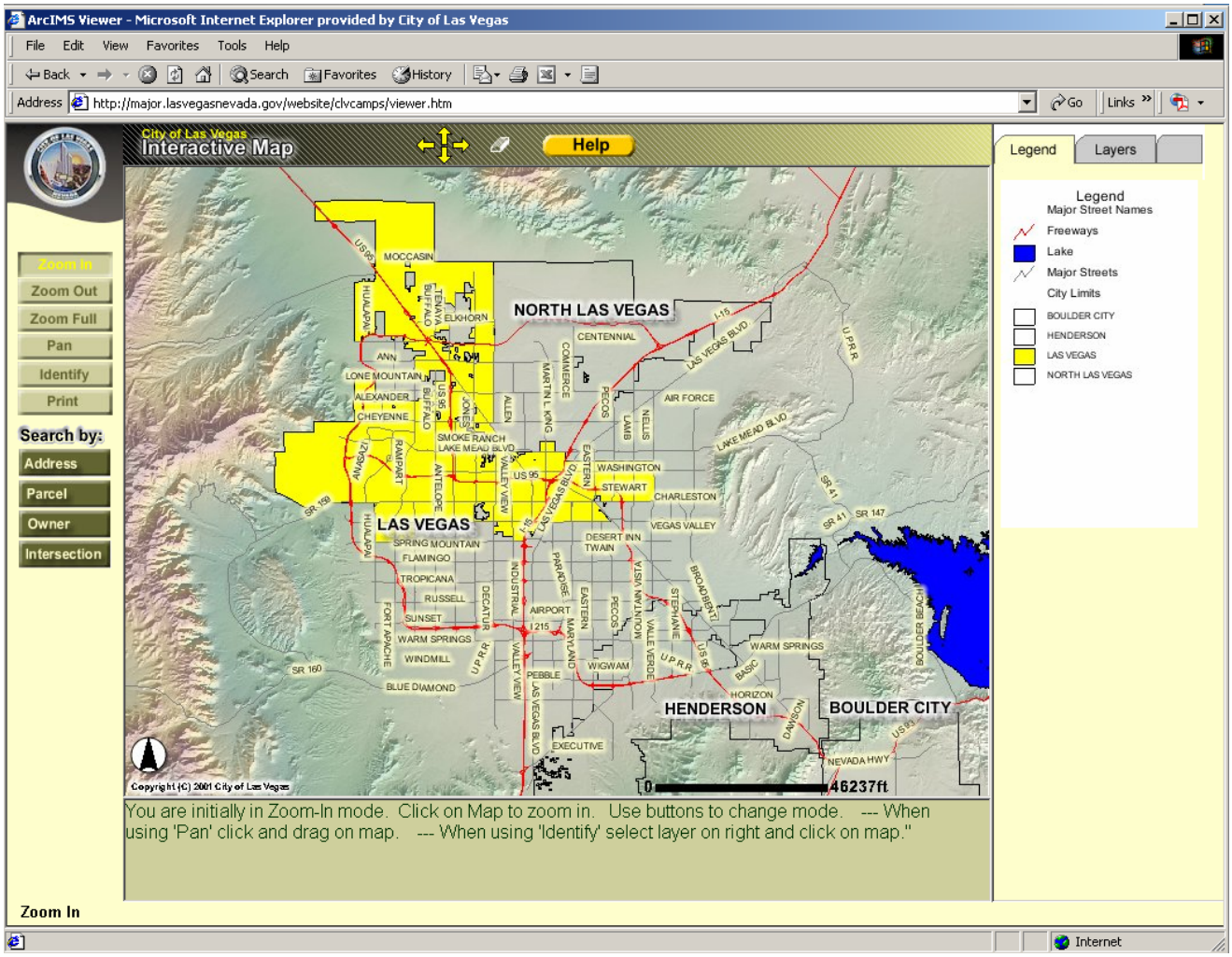
Here is an example of our I.T. Client Support Division Home Page, with a customer being highlighted and thanked for their contribution in making I.T. successful in their work area and throughout the enterprise.



APPENDIX

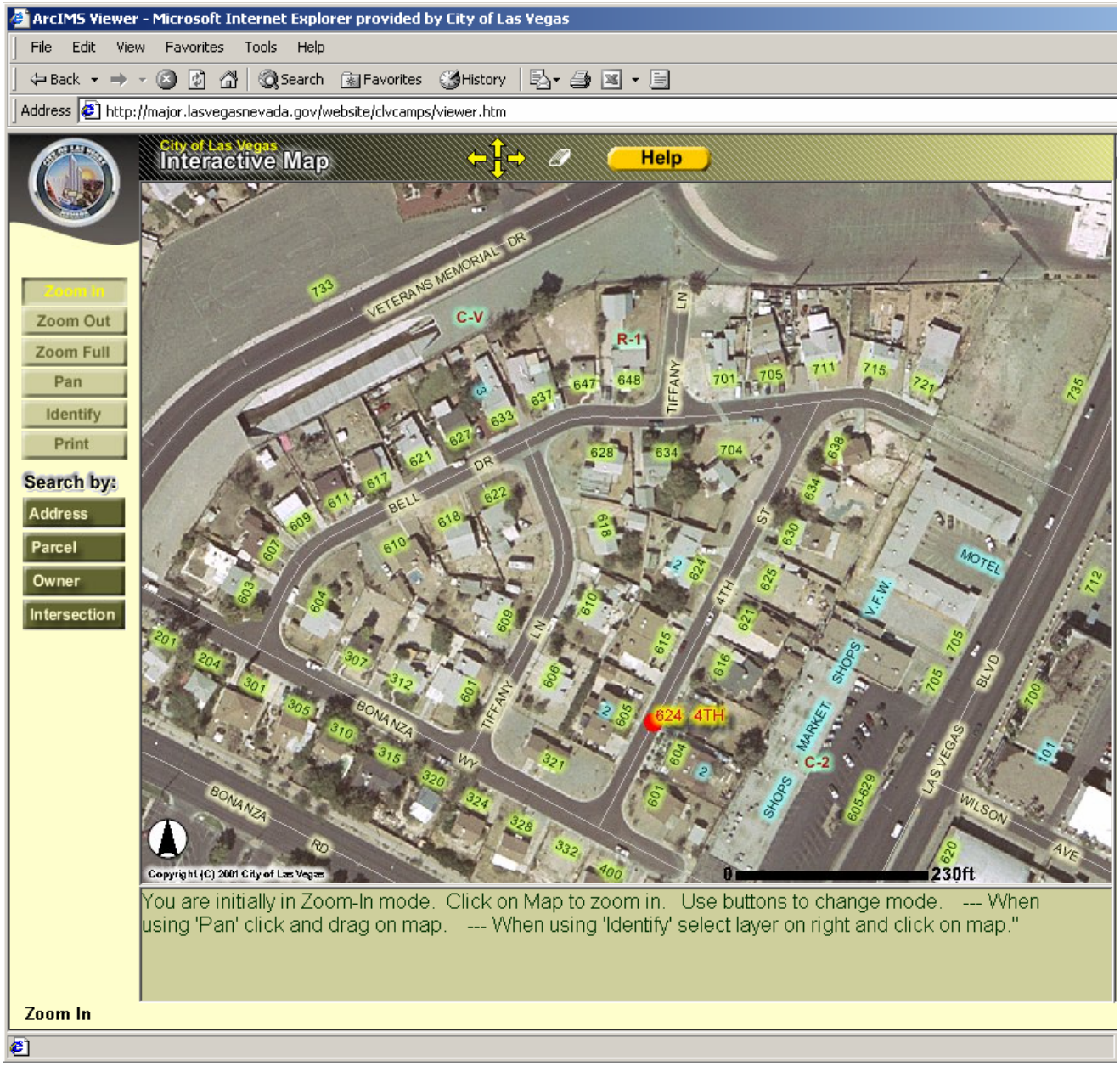
5.10 SAMPLE INTERNET GIS APPLICATION WEB PAGES

This application starts with a view of the Las Vegas Valley and then allows us to zoom in closer to a particular spot. This can be useful when trying to locate an address in relation to surrounding streets and structures.



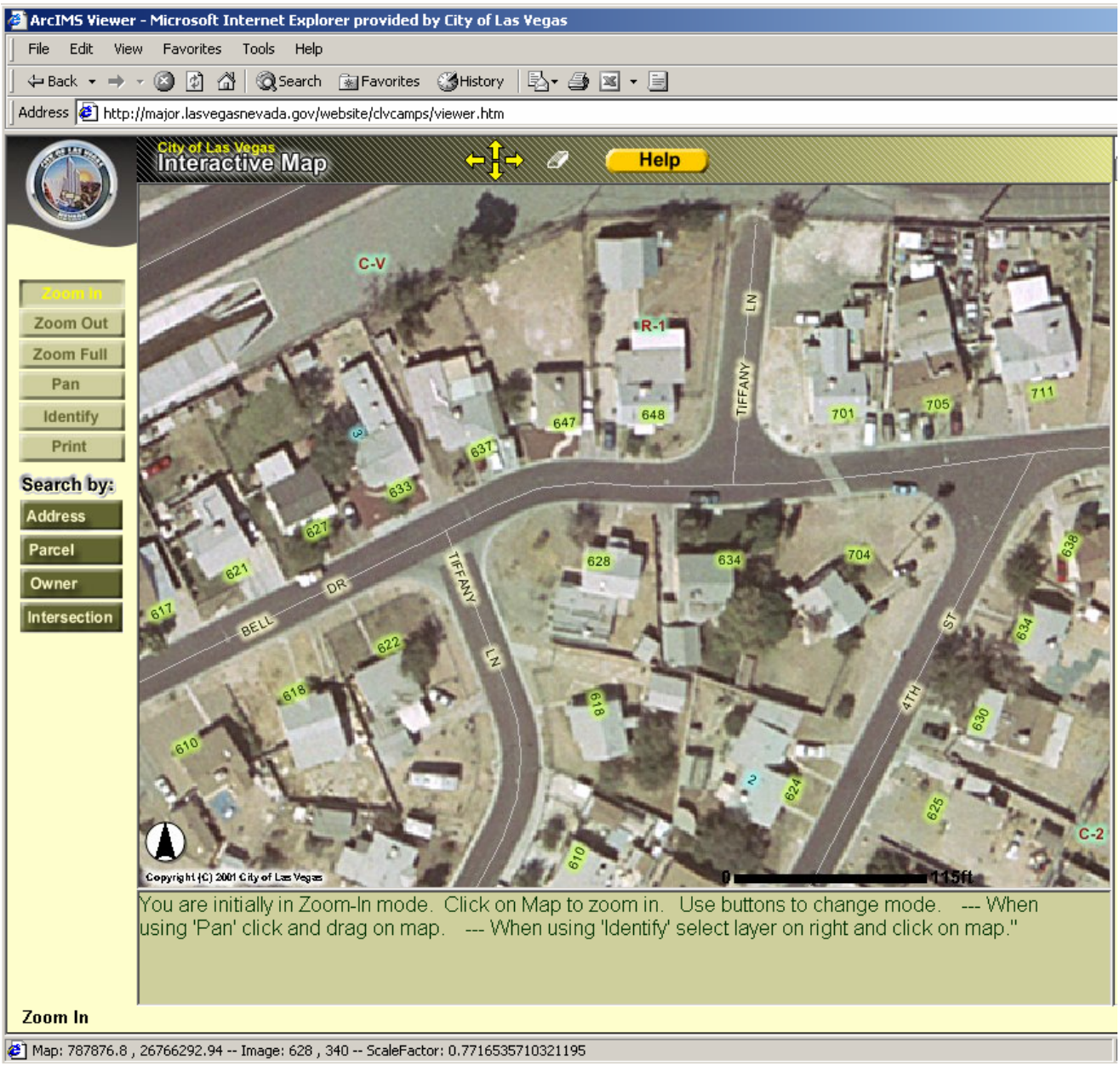
SAMPLE INTERNET GIS APPLICATION WEB PAGES

First we enter an address, which takes us closer … and …….



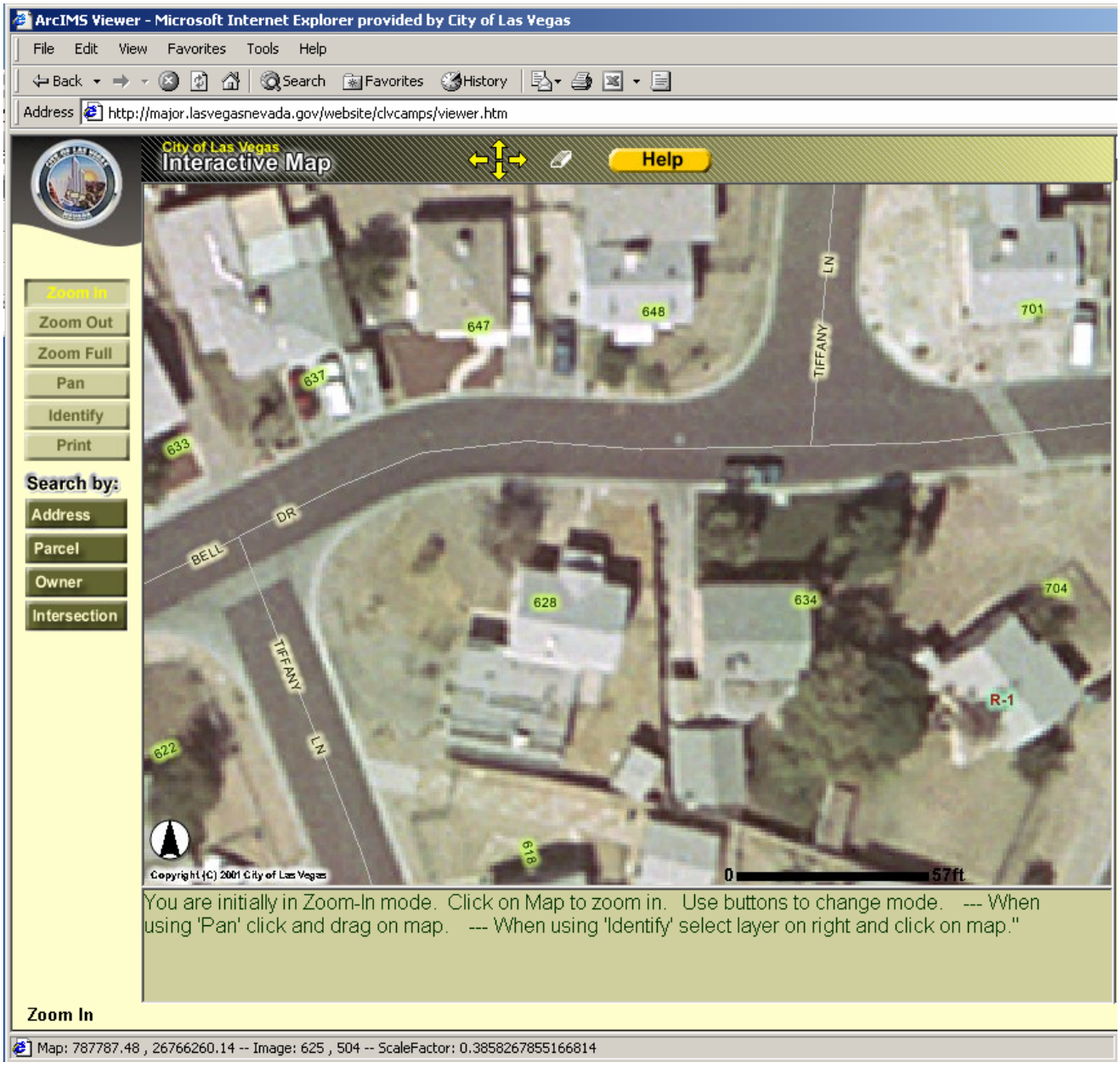
SAMPLE INTERNET GIS APPLICATION WEB PAGES

We zoom in closer……and …….



SAMPLE INTERNET GIS APPLICATION WEB PAGES

Still closer, but……



That's all for now. Thanks for your interest in I.T. Governance at the City of Las Vegas!