Information Technology Master Plan

TRANSPARENCY • PARTNERSHIP • STRATEGIC DIRECTION

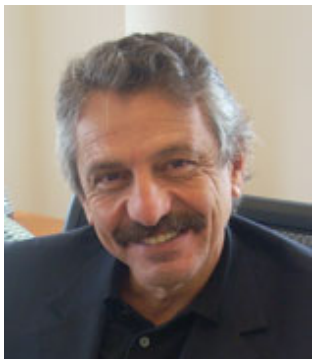
FISCAL YEARS 2009-2011

CITY OF BERKELEY

Table of Contents

Table of Contents (Continued)

Executive Summary



Phil Kamlarz, City Manager

Technology has become an increasingly critical factor in providing excellent municipal services. In Fiscal Years 2009-2011, each City department plans to enhance efficiency through process improvement, software implementation, expanded online services, and more sophisticated data analysis. In order to answer this growing demand for automation within our constrained budgetary environment, it is more important than ever that we approach technology projects with an emphasis on *standardization, integration,* and *consolidation* (see ***Principles***, page 2). Moreover, it is imperative that staff at all levels of the organization be trained to properly select, implement, and use technology tools to most effectively conduct their work.

The Department of Information Technology developed this Master Plan to provide strategic direction in equipping *"…community members and employees with innovative, secure, environmentally sound, and cost-effective technologies that facilitate excellence in municipal services, civic participation, and community well being…"* (see ***Technology Vision***, page 2) while supporting City Council's operational and administrative priorities:

- Affordable Housing
- Public Health & Public Safety
- Economic Development
- Youth & Recreation
- Environmental Stewardship
- Infrastructure & Process Improvement
- Improved Internal Controls
- Enhanced Analytical Tools

Successful technology initiatives in Fiscal Years 2005-2008 (such as computer replacement, server consolidation, enterprise licensing, and web content management) and start-up investments in powerful, state-of-the-art enterprise systems (such as Community Relationship Management and Interactive Voice Response) helped strengthen the City's technical infrastructure with shared assets that each department will leverage to further streamline business processes in Fiscal Years 2009-2011. The 35 initiatives outlined in this document reflect 5 key strategies for continuing to improve our use of technology in each City department (see ***Strategies & Goals***, page 4):

1. Broaden *community access* by upgrading the City's public computer lab, web, and telephone infrastructure.
2. Restructure *business applications* by implementing a service-oriented architecture (SOA) for software integration and scalability that maximizes return on investment.
3. Improve *data management* and *decision-making* by creating a data-warehouse that enables optimized collection, storage, and analysis of information.
4. Encourage *organizational development* by promoting technology training and purchasing as strategic investments, rather than ad-hoc activities.
5. Streamline *network operations* by updating security tools, consolidating voice and data networks, and launching a Green IT program.

With a focus on solutions that facilitate process improvement, the Department of Information Technology will continue forging strong partnerships with all departments so that the vision reflected in this Master Plan is achieved by engaging staff from all levels of the organization in determining the City of Berkeley's technology future.

Technology Vision

The City of Berkeley will equip community members and employees with innovative, secure, environmentally sound, and cost-effective technologies to provide excellent municipal services, facilitate civic participation, and help improve the day-to-day lives of community members.

Principles

Four basic principles have guided the development of this plan:

Principle 1: **Technology Investment Must Be Linked To Process Improvement.**

This plan is put together not for technology's sake, but rather for the sake of Berkeley's community. Before approving any technology initiative, we ask: *How will this help our **community members** and/or our **employees**?* If the answers are not convincing, there is no reason to move forward. When the answers are convincing, technology investment must be linked to explicitly articulated process improvements that ensure maximum return on investment. The Department of Information Technology follows a formal methodology for assessing and planning a proposed project's potential for process improvements vis-à-vis four evaluation criteria: *improved community services*, *more efficient City operations*, *greater public access to information*, and/or *more open and dynamic interaction with the public*.

Principle 2: **Standardization, integration, and consolidation are key to maintaining a scaleable technology infrastructure that maximizes return on investment.**

Standardization refers to the practice of limiting the variance across technology solutions aimed at answering the same or similar needs. ***Integration*** is the process of creating interoperability between two separate technology solutions. ***Consolidation*** refers to limiting the number of separate installations of the same or similar technical tools. A technology is ***scaleable*** when it can accommodate expansion in service scope or quantities without requiring massive platform or architectural overhauls. Scalability helps maximize return on investment (ROI) and is contingent upon a technical infrastructure that enforces optimal levels of ***standardization***, ***integration***, and ***consolidation***, across departments and business processes.

Principle 3: **Non-Baseline technology projects must be fully funded before they will be initiated.**

Baseline work refers to the routine technology services that are included in the Department of Information Technology's budget and reflect the activities that **must** get done in order to maintain the City's technical infrastructure (email, telephones, file servers, and FUND$ support). ***Non-baseline*** work includes new technology projects meant to improve specific departmental business processes, such as the Public Works Department's new transfer station and asset management systems, the Finance Department's new buisiness licensing and grant management systems, and the new Police and Fire workflow systems. The start-up costs associated with these sorts of activities must be funded by the sponsoring departments/workgroups. Once

non-baseline projects are completed, the associated maintenance costs will usually become part of the City-wide baseline technology budget.

Principle 4: **Technology Governance is an organizational imperative.**

The Technology Governance Group (TGG) was formed to ensure a Citywide approach to choosing technology investments and policies. More specifically, the TGG prioritizes "Notice of Interest" (NOI) submissions from departments interested in pursuing technology projects. The TGG comprises two permanent chairs – the Deputy City Manager and the Director of Information Technology -- and five rotating chairs open to interested Department Directors. Staff from all departments may submit a Notice of Interest (NOI) form via the DoIT service request system (submitting the NOI suggests that the appropriate Department Director has approved the project). The Director of Information Technology determines whether or not the NOI is automatically approved or requires TGG review. Once an NOI is approved, IT resources are allocated to support the project. In addition to approving individual projects, the TGG initiates important Citywide policy and operational improvements, such as Administrative Regulations and centralized data warehousing.

Strategies & Goals

This plan applies five core strategies toward achieving the City's primary technology goals:

Focus Area	Strategy		Goal
1. Community Access:	Upgrade the public computer lab, web, and telephone infrastructure.	…in order to…	Provide 24x7x365 access to routine services and help bridge Berkeley's digital divide.
2. Business Applications:	Implement a service oriented architecture (SOA) for software interoperability and scalability.	…in order to…	Maximize return on all software investments.
3. Data Management:	Create a data-warehouse for data collection, storage, and analysis technologies.	…in order to…	Improve decision making, planning, and performance measurement.
4. Organizational Development:	Promote technology training and purchasing as strategic investments, rather than ad-hoc activities.	…in order to…	Develop a technically proficient workforce skilled at using technology to deliver excellent City services.
5. Network Operations:	Implement updated security tools, consolidate voice and data networks, and launch a Green IT program.	…in order to…	Improve the security, cost-effectiveness, and environmental impact of the City's technology operations.

Technology Profile

Community

With a population of approximately 103,000, Berkeley is the 4th most populated City in Alameda County following Oakland, Fremont, and Hayward. Residents and community stakeholders represent a wide range of geographic, educational, socioeconomic, and ethnic backgrounds. As a "highly-wired" community, Berkeley's demand for online tools and 24x7 access to government is higher than might be found in most communities.

Network Infrastructure

The City of Berkeley's wide area network (WAN) comprises a local area network (LAN) gigabit fiber connection through 3 central buildings (2180 Milvia Street, 1947 Center Street, and 2100 Martin Luther King Way) and 19 T1 lines that connect remote offices to the City's Central Data Center (CDC). This network serves all 28 City geographical locations and uses a mixture of transport layers, including fiber optic cable, CAT 6/5e UTP, T-1 digital lines, a point-to-point 802.11a wireless system, and cellular EVDO connectivity. The switching infrastructure is standardized on Cisco devices. The data storage infrastructure is built upon EMC network attached storage (NAS) and storage area network (SAN) equipment.

Servers

The City of Berkeley's server inventory consists of 105 servers with an average age of six years. The core financial and public safety systems run on two IBM AS400s; nearly all other servers run Microsoft Windows Server 2003 on Dell hardware. In accordance with the City's commitment to environmental stewardship, the Department of Information Technology aims to consolidate at least 30 of these servers by Fiscal Year 2011 using "virtual servers" that consume less energy and cost less to maintain.

Desktops, Laptops, & Monitors

The City of Berkeley's computer inventory comprises 1,202 desktop computers, 106 general-purpose laptops, 55 Public Safety (Police and Fire) ruggedized laptops, and 1,227 computer monitors (there are more monitors than staff computers because some desktop systems use multiple monitors). In Fiscal Year 2007, the standard desktop configuration for new system purchases changed from a large "tower" configuration to a "small form factor" which saves space and is more energy efficient. The average age of the City's desktop systems is approximately 4.8 years. Nearly all desktop computer systems run the Microsoft Windows and Microsoft Office, though there is still an undesirable and inefficient level of non-standardization (Microsoft Operating Systems: *3%=Windows 98, 20%=Windows 2000, 75%= Windows XP, 2%=Windows Vista test machines*; Microsoft Office Suite: *2%=Office 98, 94%=Office 2000; 1%=Office 2002 (XP); 2%=Office 2003; 1%=Office 2007 test machines*). By Fiscal Year 2011, the Department of Information Technology aims to standardize 99% of all staff computers on the same Microsoft Windows operating system and Microsoft Office suite. This will not only permit reallocation of IT staff support time to more complex project work, but also make information exchange amongst Citywide staff more efficient.

Printers, Scanners, Multifunction Copiers

The City's inventory of networked printers includes 102 black and white laser printers, 12 color laser printers, 29 color inkjet printers, 3 impact (dot matrix) printers and 8 color plotters (for large format prints). There are also over 230 desktop printers, 3 stand-alone document scanners, and 11 multifunction copiers that combine the functions of copying, printing, scanning, and faxing. The multifunction units are more cost effective than single function printers. By Fiscal Year 11, the number of desktop printers and stand-alone scanners will decrease by at least 25% in favor of the more cost-effective and environmentally friendly multi-function units.

Software

Major software applications at the City of Berkeley fall into four categories: **Enterprise Applications** that all City Departments depend upon and, therefore, form the 'core' of our software infrastructure; **Departmental Applications** that one or a few City departments rely upon to guide specific business processes; **Desktop Applications** that reside on the standard City computer image; and peripheral or **Task Applications** that are used for specific functions that are usually ancillary to core business activities. The relationship amongst enterprise applications, as well as between enterprise and departmental applications, has been inconsistent due to incompatible technologies and decentralized software selection. In Fiscal Year 2008, the Department of Information Technology implemented a centralized middleware framework to maximize interoperability and minimize development costs, and expedite development cycles. By Fiscal Year 2011, the number of individual peripheral applications will drastically decrease as they are consolidated into centralized enterprise or departmental applications.

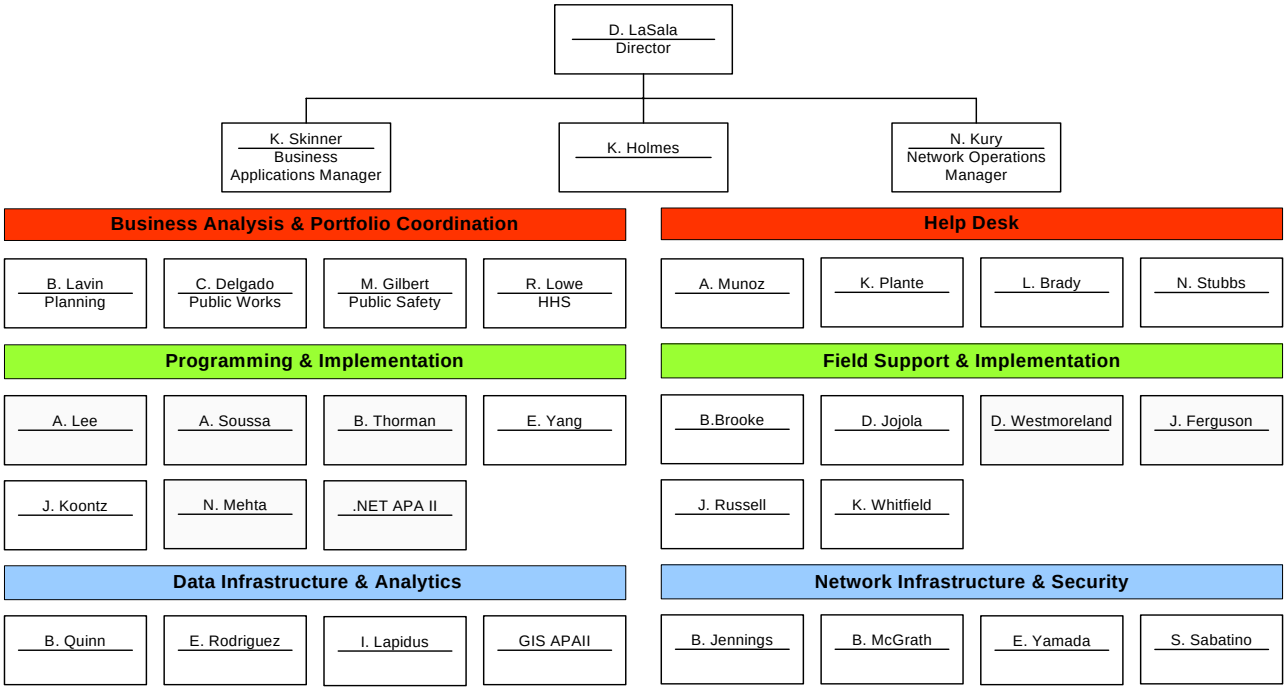
Technology Staff

Prior to Fiscal Year 2003, it was common for departments to hire and manage technology staff outside the Department of Information Technology. From Fiscal Year 2003 to Fiscal Year 2008, almost all technical staff were centralized to correct inefficiencies created by the technology silos that had developed, and the City placed high priority on creating a properly administered central technology program.

As of Fiscal Year 2009, there are 33 full time permanent information technology positions throughout the City. Since Fiscal Year 07, the number of Information Technology managers decreased from five to three, and the associated funding was reallocated to hire three additional technicians (two programmers and one network security officer).

Citywide Information Technology Staffing

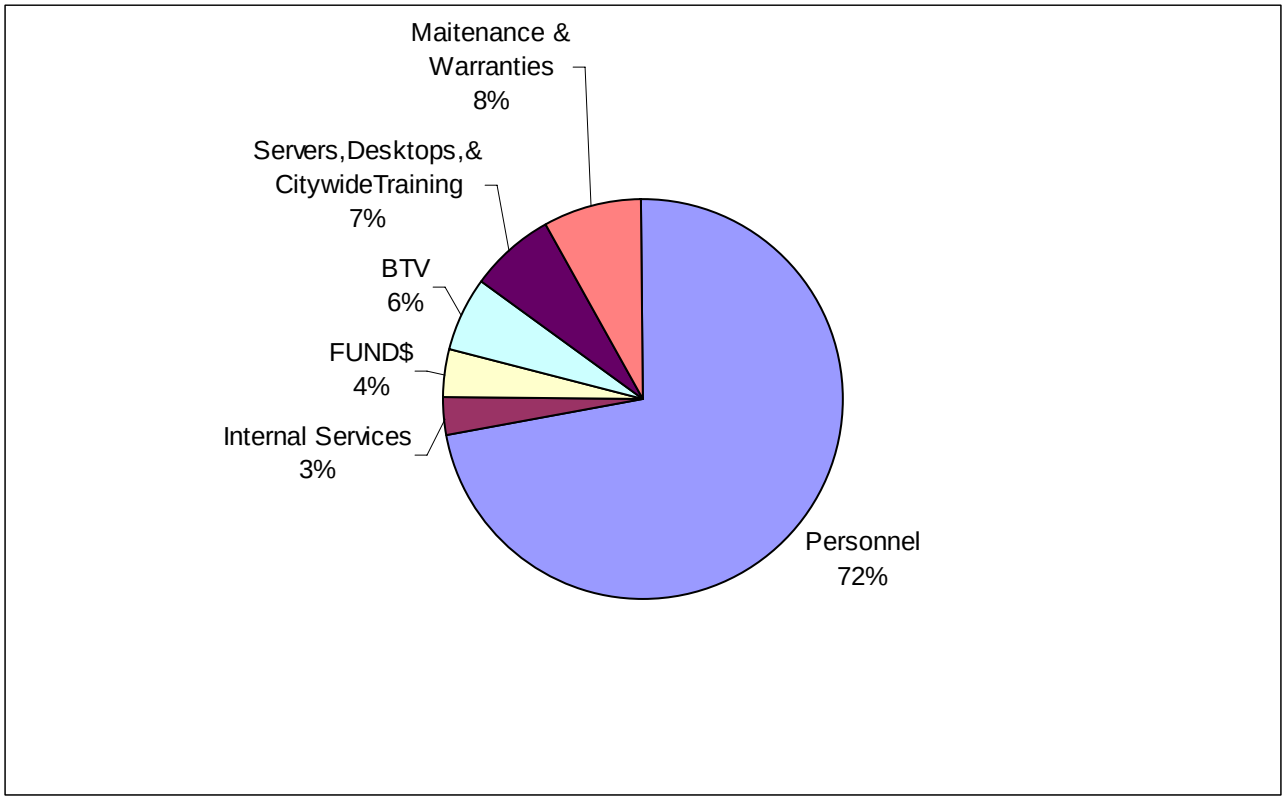
FY 09: 33 Full Time Employees



Technology staff members are assigned to a combination of ***baseline*** and ***non-baseline*** activities (see ***Principles***, page 2) and work together as a team to:

- Maintain an efficient and effective technology infrastructure.
- Strengthen internal controls and security throughout the City's technology infrastructure.
- Ensure that baseline technology systems are recoverable in disaster situations.
- Appropriately balance the need to minimize risk, operate with limited resources, and facilitate the rapid exchange and analysis of information.
- Encourage the appropriate use of technology to support City Council priorities and improve Departmental business processes.
- Deliver quality services that are valued by City staff and the Berkeley community.

Technology Budget



The FY 2009 Department of Information Technology (DoIT) baseline budget totals **$4,350,165**:

• Personnel Costs	$3,132,120	72%
• Maintenance & Warranties	$ 348,013	8%
• Servers, Desktops, & Citywide Training	$ 304,511	7%
• Berkeley Community Media (BTV)	$ 261,010	6%
• FUND$ Support	$ 174,006	4%
• Internal Services	$ 130,505	3%
	$4,350,165	

The Department of Information Technology's baseline budget funds ***baseline*** work - routine technology services that **must** get done in order to maintain the City's technical infrastructure (email, telephones, file servers, FUND$ support, and maintenance of critical systems).

Non-baseline work includes new technology projects meant to improve specific departmental business processes, such as the Public Works Department's new transfer station and asset management systems, the Finance Department's new business licensing and grant management systems, and the new Police and Fire workflow systems. Sponsoring departments must fund the costs associated with these sorts of activities. Once such non-baseline projects are completed, they are candidates for inclusion as part of the City's baseline technology infrastructure. In such cases, associated maintenance costs will usually become part of the Department of Information Technology's baseline technology budget.

Policies

Threats to computer network security are on the rise each year due to increasing reliance upon computer-based technology, widespread Internet connectivity, and bad habits with regard to the use of technology. The Department of Information Technology - - in cooperation with the City Manager, the Technology Governance Group, the Department of Human Resources, and the City Attorney - - has established the following polices aimed at protecting the City of Berkeley's information and technology assets from threats associated with unauthorized access, inappropriate use, information leakage, denial of service, data integrity, and natural disasters:

I. Administrative Regulation 4.2: Computer Network Resources

PURPOSE: The City of Berkeley ("City") provides various computer network resources to authorized employees to assist them in performing their job duties for the City. Each employee has a responsibility to use such City resources in a manner that increases productivity, enhances the City's public image, and is respectful of other employees. This administrative regulation sets forth the City's policy regarding the use of and access to the City's computer network resources, including but not limited to the City's electronic communication, workflow, data storage, and business application systems, hardware (including connected and disconnected computers, servers, switches, routers, etcetera), software, electronic mail ("email"), access to the Internet and World Wide Web, voice mail, and any data thereon (hereafter collectively "Computer Network Resources").

This administrative regulation applies to all employees (temporary or permanent), City officials or other authorized City users such as consultants (hereafter "Employees") other than patrons of the Berkeley Public Library ("Library") with respect to their access to Library computers assigned for public use. The City's Computer Network Resources are City property, regardless of physical location or the form in which they are maintained, and are to be used for City business in the course of normal operations.

The City reserves the right to change the policies and procedures set forth in this administrative regulation at any time.

Employees should be aware that all records, whether on paper, voicemail, or computerized, are subject to the mandatory public disclosure requirements of the Public Records Act, subject to the exceptions provided under the Act. In addition, Employees who use the City's Computer Network Resources do so with no right or expectation of privacy or confidentiality, and at all times the data, systems, and traffic they create utilizing the City's Computer Network Resources remain the property of the City.

Violations of this administrative regulation subject Employees to discipline up to and including termination. In the event of a violation, the City may pursue all remedies provided under the law, including advising legal and/or law enforcement authorities of any violation of law by an Employee.

POLICY: The City's Computer Network Resources are City property, regardless of physical location or the form in which they are maintained, and are to be used for City business in the course of normal operations. Employees who use the City's Computer Network Resources do so with no right or expectation of privacy or confidentiality. The use of all Computer Network Resources must comply with all requirements set forth in this administrative regulation and all other City policies, including but not limited to Administrative Regulation 3.17 ("Fraud, Abuse and Misuse of City Resources"). While passwords are issued to Employees in order to protect the City's business interests and to limit access to certain City information, the conferral of such passwords does not create any individual right of privacy in any such Employee as to the City's Computer Network Resources, including any data, files, or messages sent to, received, or created by such Employee.

CITY RIGHTS:

- The City has the capability to and may, with or without notice for any lawful purpose, monitor and audit all network activity to ensure compliance with this administrative regulation, and activate, access, block, review, copy, disable, delete, and/or disclose any information residing on any Computer Network Resources, including, but not limited to emails sent and received, voice mail messages received, files created or accessed, and all internet/web access, communications, and transactions.

- The City Manager has the right to access all Computer Network Resources and may authorize the Director of Information Technology to access any and all Computer Network Resources for any legitimate City business reasons, including to ensure appropriate use of the City's Computer Network Resources and/or to determine compliance with this administrative regulation. The City reserves the right to access, delete, or retain any Computer Network Resources at any time.
- In order to protect the City's privacy and confidentiality interests and to ensure the security of the computer network, the City provides Employees with individual password protection; these passwords do not confer any right or expectation of individual privacy.
- The City Manager and each department director have the right to ask for and receive all Employee passwords within the department. Each department director has the right to inspect any and all Computer Network Resources of the department's Employees to correct service problems, ensure system security, retrieve records, and/or transition work when responsible personnel are unavailable, and for other legitimate City business reasons.
- Data residing on Computer Network Resources is purged on a regular basis and the City may, at its discretion, purge any such data on an automatic basis without notice.

RULES - General Rules Applicable To The Use Of All Computer Network Resources:

The rules described below are provided as examples, and are not intended to be an exhaustive list. Unless an Employee is exempted from following one or more of these rules by prior written permission by either the City Manager or the Director of Information Technology, failure to abide by these rules shall subject an Employee to disciplinary action, up to and including termination.

- Employees shall use Computer Network Resources solely for official City business, which may include scheduling work-related social events such as lunches, retirement parties, birthdays and bereavement notices.
- Employees are prohibited from using Computer Network Resources to access or transmit information that is threatening, defamatory, obscene, discriminatory, offensive, or in violation of the City's Harassment Prevention Policy, or any other City policy. Such prohibited use shall be punishable by severe disciplinary action, up to and including termination.
- Employees, and unions representing City employees, are prohibited from using the City's Computer Network Resources to conduct membership business, *i.e.*, to inform its members of union business. Employees, and unions representing City employees, may use the City's Computer Network Resources to communicate with the City regarding grievances, labor negotiations or other matters to which the City is a party.
- Electronic snooping or tampering is a violation of this administrative regulation and is grounds for disciplinary action, up to and including termination. This includes but is not limited to the unauthorized use or attempt to use another employee's password without the employee's consent; the unauthorized entry to or attempted entry to the computer files and communications of another without that person's consent; the unauthorized entry or attempted entry to access encrypted, protected, or restricted Computer Network Resources for which an Employee has not been explicitly authorized to access; unauthorized "interception" of data not intended for that person; the utilization of City data for purposes other than those related to legitimate City business within the scope of direct job duties (including the use of public domain data obtained without following appropriate public information request procedures); or any other attempt to circumvent user authentication or security of any computer network resource.

- Employees shall not create or transmit fraudulent or damaging information, including, but not limited to, forged or modified email header information; malicious programs (e.g., viruses,

worms, Trojan horses, e-mail bombs, etc.), or fraudulent offers of products or services from any City account.

- Employees are prohibited from accessing entertainment websites, software, or games, including participation in Internet gaming and dating sites, and may not use or download files for personal purposes, including but not limited to formats such as .MP3, .WAV, .EXE and .AUD.

- Employees are prohibited from activating port scanning, security scanning, or workstation firewalls unless prior written permission of the Department of Information Technology is obtained.

- Employees shall protect network security by regularly changing individual passwords in accordance with IT guidelines, and are prohibited from sharing individual passwords with others except as provided herein for legitimate City business.

- Employees may forward or re-distribute copies of email messages only when doing so fulfills a legitimate business need of the City, and are prohibited from sending mass email messages to employees outside of the established “Everyone Email” process, which requires approval of the City Manager. Employees shall not create or forward "chain letters", "Ponzi" or "pyramid" schemes, or send unsolicited email messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (spamming).

- Misaddressed email shall be returned to the sender with an explanation of the error, and then deleted. However, if the misaddressed email is offensive, inappropriate, or otherwise in violation of this administrative regulation, the misaddressed email shall be forwarded to the recipient's department director, or the Director of Information Technology, for appropriate action.

- Email is not a permanent storage medium and staff is prohibited from using it as such. The City stores email for a limited period, only to recover current email in the event of a systems failure.

- Employees may not transmit, obtain or access information in violation of any federal, state or local law, ordinance or regulation, including copyright laws and/or transmit, obtain, or access files or communication for any unlawful purposes.

- Employees are prohibited from installing unauthorized computer programs, including but not limited to Really Simple Syndication (“RSS”) feeds or similar technology, games, screen savers, and email add-ons such as animated “smiley faces” or backgrounds.

- The City may authorize persons who are not employed by the City to use the City's Computer Network Resources, only after such person makes a written request to the appropriate department director or to the City Manager. Such authorized access may be granted only upon the condition that such person shall use the system according to the rules and procedures established in this administrative regulation and all other City policies.

Rules Regarding Passwords & Access:

- Passwords are issued to Employees in order to protect the City's network security and business interests and to create limited access to certain City information. The conferral of such passwords does not create any individual right of privacy in any such Employee as to the City's Computer Network Resources, including any data, files, or messages sent to, or received or created by such Employee.
- Authorized users are responsible for the security of their passwords and accounts. FUND$ passwords must be changed quarterly; network domain passwords must be changed every six months. Employees are prohibited from posting passwords in a location that is visible to, or accessible by, others.
- Each Department Director, or a person designated by a Department Director, has the right to obtain all departmental employee passwords; Employees are not permitted to share individually assigned passwords with any other person.

Rules Regarding Hardware & Software:

- Only approved hardware and software is permitted on the City's network. Personally owned hardware, software, and data are prohibited from the City's network, unless written permission is obtained from the Director of Information Technology via a formal service request. Employees shall not install or activate any copyrighted software for which the Department of Information Technology has not confirmed an active license.
- All hardware with the potential or capacity to access Computer Network Resources (including but not limited to PCs, laptops, servers, handhelds, and wireless devices) is required to be secured with a password-protected screensaver.
- All hardware with the potential or capacity to access Computer Network Resources must run virus-scanning software approved by the Department of Information Technology. Users are prohibited from interfering with the effective operation of the City's approved virus-scanning software, or any other network security or network monitoring system installed by the Department of Information Technology.
- Employees authorized to use portable computers (laptops, wireless devices, handhelds, blackberry units, cell phones, *et cetera*) must adhere to all applicable guidelines to protect those vulnerable devices.
- Employees are prohibited from adding external hard drives to any City computer, unless those drives are approved, in writing, for a specific use by the Director of Information Technology via a formal service request.
- Employees are prohibited from using encryption tools other than those approved by the Department of Information Technology.

- Unless otherwise authorized, in writing, by the Department of Information Technology via a formal service request, all employee workstations are to be set in "administrator lockdown" mode.
- Employees are not permitted to use workstations, network drives, or other devices outside the City's server rooms as application servers, data servers, or other workgroup access points unless authorized, in writing, by the Director of Information Technology via a formal service request.
- All software on the City network must be properly licensed. The Department of Information Technology, in accordance with the City's software inventory procedures, must centrally maintain all software media, licensing information, and access codes.
- Software and hardware purchased by the City is intended for City business only.

Computer Network Access - Department Responsibilities:

The following steps are required to activate, transfer, or disable network access for new employees, transferring employees, and/or terminated employees:

- The responsible Department Director or Supervisor must submit a service request to the Department of Information Technology at least five (5) business days prior to the required action.
- In the case of account activation, the Department of Information Technology will confirm the new account and provide a password directly to the employee.
- For individuals who are not permanent City employees, the responsible Department Director, or designee, is required to specify and uphold the expected duration of access.
- When an employee is separated from service, the Department Director or Supervisor must notify the Department of Information Technology, obtain all employee passwords, and copy any files to be retained. The Department of Information Technology will delete accounts, systems, and data unless requested to do otherwise by the Department Director.

II. Training and Awareness Policy

PURPOSE: To establish security awareness and education requirements for all workforce members.

All workforce members who have been granted access to City of Berkeley Computer Network Resources, including but not limited to full and part-time employees, temporary workers, volunteers, contractors, those employed by others to perform City of Berkeley work, and others granted access, are covered by this policy and shall comply with this and associated policies, procedures and guidelines.

Security awareness and education program ownership:

- In cooperation with the Human Resources Department Training Officer, DoIT will manage an information security awareness and education program for the City workforce.
- By December 2008, all employees will have online access to CoB Security Policies and the AR 4.2 Acknowledgement Form.

Security awareness and education program contents:

- The information security awareness and education program covers information security basics, associated policies and procedures, and workforce member responsibilities.
- The information security awareness and education program also includes specific information on the use of security precautions such as encryption, anti-viral tools, backup procedures, physical security and awareness of social engineering tactics.
- DoIT will continue to post current information security best practice guidelines and related documents on the City's Intranet.

AR 4.2 Acknowledgement Form:

- City of Berkeley employees shall acknowledge they have been informed and are aware of City of Berkeley Information Security policies, and their role in protecting City of Berkeley information systems and information assets, by signing the AR 4.2 Acknowledgement Form.
- The City of Berkeley Office of Human Resources shall be responsible for the collection and management of signed AR 4.2 Acknowledgement Forms.

Security awareness and education for contractors and partners:

- The City of Berkeley requires contractors and partners to sign the Third Party Agreement Form in order to establish their role in protecting City of Berkeley information systems and information assets.
- City of Berkeley information security awareness and education materials shall be made available for use by contractors and partners for the education of their workforce members who have access to City of Berkeley information systems and information assets.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REVISION HISTORY

1/1/08
5/15/08
7/15/08

III. Network Access Policy

PURPOSE: This policy outlines rules that govern granting and maintaining onsite and remote access to the City of Berkeley's Computer Network, including the creation of user accounts, standards for connecting to the City of Berkeley's network from any Internet host, and the conditions under which third party organizations may use an extranet connection to the City.

Access to the City of Berkeley Network is managed and controlled through security systems and audit trail monitoring. Any effort to circumvent security systems or auditing tools - - or to exploit any known or unknown vulnerabilities - - will be regarded a security breach in violation of Administrative Regulation 4.2 and shall be handled accordingly.

USER ACCOUNTS

DoIT ensures that all employees, agents, contractors, consultants, et cetera use Unique User IDs and passwords to gain authorized access to the City of Berkeley's information assets.

1. Account Creation: DoIT will create a new user account only in response to a properly submitted electronic Service Request. DoIT will create the account such that the user is forced to change the initial password in order to login to the network (see the Password Policy).
2. Unique User Identification (ID): Each authorized user shall be assigned a Unique User ID for which that user shall be held responsible and accountable for the purpose of initiating the login process to the City of Berkeley's information systems. The Unique User IDs are not to be shared with other users for the purpose of gaining access to the City of Berkeley's Computer Network Resources. Authorized users shall be held accountable and responsible for the use and activity of assigned Unique User ID.
3. Granting User IDs to Outsiders: Contractors, consultants and other non-employees may be granted a User ID in response to a properly submitted electronic Service Request.
4. Account Formats: User IDs are intended to facilitate easy identification of the individuals to whom they are assigned. A particular User ID is based on the name that appears on official City of Berkeley employment records.
    - The format of the User ID is derived from the user's first name initial followed by their last name (e.g., Jane Doe = jdoe). Since no two users can have the same ID, potential duplicates are resolved by adding a middle initial, or, if no middle initial exists, using the second letter of the user's first name.
    - Spaces are not permitted in User IDs, so last names that consist of multiple words will be treated as if one word (e.g., De La Garza = delagarza). Since hyphens are permitted in User IDs, last names separated by hyphens are not altered when assigned a User ID.
    - Note: The fact that a "first" name may consist of multiple words is irrelevant for the purpose of User ID assignment, because only one initial is derived from the first name (e.g., Billy Ray Smith = bsmith, NOT brsmith).
    - Exceptions and Changes: Any deviations from the User ID standards outlined herein must be requested of the Department of Information Technology in writing via service request, clearly stating the reasons an exception is needed.
5. Termination: User access will be terminated in response to a properly submitted electronic Service Request. As a check against the possibility of terminations that do not have an associated

Service Request, DoIT compares Human Resources' Termination List against its list of active user accounts. DoIT revokes the access rights of individuals who appear on both lists.

REMOTE ACCESS

Remote access includes, but is not limited to, dial-in and cable modems, frame relay, ISDN, DSL, VPN, SSH, etc. These standards are designed to minimize the potential exposure to the City of Berkeley from damages that may result from unauthorized remote use of City of Berkeley resources. Damages include the loss of confidential or otherwise sensitive data, the loss of intellectual property, damage to public image, damage to critical internal systems, etc.

Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for City of Berkeley or to the Public Switched Telephone Network does NOT fall under this policy. Users who will be accessing the City of Berkeley's network remotely must do so in accordance with Administrative Regulation 4.2. Remote access to the City's computer network is granted in response to a documented DoIT Service Request. Under no circumstances is a remote access conduit permitted without the express approval of the Department of Information Technology. Additional information regarding and technical support for remote access to the City of Berkeley's network can be obtained from the Help Desk at 981-6525.

GENERAL REQUIREMENTS:

- Secure remote access must be strictly controlled. Control will be enforced via password authentication or public/private keys with strong pass-phrases.
- City of Berkeley employees are prohibited from sharing login and password information to anyone other than a Department Director.
- Individuals with remote access privileges must ensure that, while their City-owned or personal computer (or similarly-capable device) is remotely connected to City of Berkeley's network, it is not simultaneously connected to any other network.
- Individuals with remote access privileges to City of Berkeley's network must not use non-City of Berkeley mail accounts (e.g., Hotmail, Yahoo, AOL), or other external resources to conduct City of Berkeley business.
- Routers for dedicated ISDN lines configured for access to the City of Berkeley network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is prohibited at all times.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- All hosts that are connected to City of Berkeley internal networks via remote access technologies must use up-to-date anti-virus software approved by the Department of Information Technology (this includes personal computers). Third party connections must comply with requirements as stated in the Third Party Agreement.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the City of Berkeley production network must obtain prior approval from the Director of Information Technology.

REQUIREMENTS SPECIFIC TO VPN (VIRTUAL PRIVATE NETWORK):

- It is the responsibility of employees with VPN privileges to protect those privileges from unauthorized use.
- VPN use is to be controlled using either a one-time, randomly generated credential (i.e., token) or a public/private key system with a strong pass phrase.
- When actively connected to the City of Berkeley network, VPNs will force all traffic to and from the remote client through the VPN tunnel: traffic originating from anywhere other than the tunnel's two terminals cannot access the tunnel.
- VPN gateways will be set up and managed by the IT Department's Network Operations Division.
- VPN users will be automatically disconnected from City of Berkeley's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Only DoIT-approved VPN clients may be used.

REQUIREMENTS SPECIFIC TO EXTRANET CONNECTIONS:

- Security Review: All newly proposed extranet connectivity will go through a security review by DoIT. The reviews are to ensure that all access matches the business requirements in the best possible way, and that the principle of least access is followed.
- Third Party Agreement: All new connection requests between third parties and the City of Berkeley require that the third party and City of Berkeley representatives agree to and sign the Third Party Agreement. This agreement must be signed by an authorized representative of the Sponsoring Department as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into City of Berkeley labs are to be kept on file with the DoIT Security Officer.
- All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by the Director of Information Technology. Lab connections must be approved by the DoIT Security Officer. Typically this function is handled as part of the Third Party Agreement.
- Point Of Contact: The Sponsoring Department must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Department, and is responsible for those portions of this policy and the Third Party Agreement that pertain to it. In the event that the POC changes, the relevant extranet Organization must be informed promptly.

ESTABLISHING EXTRANET CONNECTIVITY

- Begins with a DoIT Service Request: Sponsoring Departments within City of Berkeley that wish to establish connectivity to a third party are to complete a DoIT Service Request. Within the Service Request, the Sponsoring Department must provide full and complete information as to the nature of the proposed access.
- Is based on the principle of least-access: All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In

no case will the City of Berkeley rely upon the third party to protect the City of Berkeley's network or resources.

MODIFYING OR CHANGING EXTRANET CONNECTIVITY AND ACCESS

- Requires a valid business justification: All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via enterprise change management processes. The Sponsoring Department is responsible for notifying the DoIT Security Officer when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

TERMINATING EXTRANET ACCESS

When access is no longer required, the Sponsoring Department within the City of Berkeley must notify DoIT, and then DoIT will terminate the access. The Security Officer must audit all extranet connections on an annual basis to ensure that they are still needed, and that the access provided is appropriate to the business justification. Connections that are found to be in disuse will be terminated immediately. Regardless of the reason, when DoIT terminates or modifies an Extranet connection, the POC will be notified.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Vendors found to have violated this policy may be considered in breach of contract.

REVISION HISTORY

1/1/08
5/15/08
7/1/08

IV. Password Policy

PURPOSE: Passwords provide the first line of defense against unauthorized access to City of Berkeley Computer Network Resources. As such, logging into the City network requires "strong" passwords that must be changed regularly. In addition, credentials used by programs to access a City of Berkeley database must be stored and retrieved securely.

Failure to create a password that meets the strong password criteria will result in the inability to log in to the network, Fund$ or other applicable Computer Network Resource. Users of HTE's QRep and/or those who download from Fund$ to spreadsheets or text files will have to match their Fund$ and network passwords.

Passwords are not to be stored in readable form in locations where unauthorized persons might discover them. Passwords are required to be strong and are required to be changed every 6 months. Strong (and weak) passwords are described below. These descriptions are provided to employees during Core IT Training, and they are posted on the City of Berkeley Intranet.

STRONG PASSWORDS:

- Contain at least eight (8) characters
- Contain both upper and lower case letters
- Contain digits and punctuation symbols, as well as letters. Acceptable punctuation symbols include: $ (dollar sign), @ (at sign), # (number sign), and _ (underscore)
- Do not contain your user name, real name, or organization name
- Do not contain a complete dictionary word
- Are significantly different from previous passwords. Passwords that increment (e.g., Password1, Password2, Password3) are not strong.
- Change every 6 months

STRONG FUND$ PASSWORDS:

- Contain At least eight (8) but no more than ten (10) characters.
- Cannot start with a number
- Contain letters, digits and symbols (like $, @, #, and _).

WEAK PASSWORDS:

- Personal information such as your name, phone number, social security number, birth date, or address (even names of acquaintances should not be used)
- Any word in the dictionary, or based closely on such a word (such as a word spelled backwards)
- A word with letters simply replaced by digits. For example, bl0wf1sh is not a strong password
- Passwords that never change

DATABASE PASSWORDS

To maintain the security of the City's internal databases, access by software programs must be granted only after authentication with credentials. Those credentials must not reside in the main, executing body of the program's source code in clear text. In addition, database credentials must not be stored in a location that can be accessed through a web server.

SPECIFIC DATABASE REQUIREMENTS

1. Storage of Data Base User Names and Passwords:
   - Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world-readable.
   - Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
   - Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
   - Database credentials may not reside in the documents tree of a web server.
   - Pass-through authentication must not allow access to the database based solely upon a remote user's authentication on the remote host.
   - Passwords used to access a database must adhere to the strong password guidelines described above.
2. Retrieval of Database User Names and Passwords:
   - If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
   - The scope into which database credentials may be stored must be physically separated from the other areas of code—that is, the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
   - For languages that execute from source code, the credentials' source file must not reside in the same browse-able or executable file directory tree in which the executing body of code resides.
3. Access to Database User Names and Passwords:
   - Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

ENFORCEMENT

As stated above, failure to create a password that meets the strong password criteria will result in the inability to log in to the network, Fund$ or other applicable Computer Network Resource. An individual who cannot complete assignments due to the failure to create an acceptable password may be subject to disciplinary action, up to and including termination of employment. Those experiencing difficulty with password creation are directed to contact the DoIT Help Desk at 981-6525. Additionally, an individual who circumvents the database security provisions of this policy may be subject to disciplinary action, up to and including termination of employment.

REVISION HISTORY

12/31/07
5/15/08

V. Internet Filtering Policy

PURPOSE: The purpose of this policy is to mitigate the City's exposure to legal, security, and bandwidth risks.

Access to the Internet is filtered using automated software and regularly audited in order to mitigate legal liability, safeguard network operations, and optimize bandwidth. This policy applies to all City of Berkeley employees, contractors, consultants, and other workers including all personnel affiliated with third parties utilizing the City of Berkeley's Internet and network bandwidth.

Sworn Police Department staff may receive limited exceptions to this policy for investigative purposes, based on written authorization by the Director of Information Technology in response to a written request from the Chief of Police.

The types of websites that fall into the risk categories listed above are discussed with employees during Core IT Training classes and summarized on iCoBWEB, the City of Berkeley Intranet. They include, but are not limited to:

LEGAL RISK:

Sex	Gambling
Personals & Dating	Pornography
Hate	

BANDWIDTH SATURATION RISK:

Personals & Dating	Internet Radio & TV
Internet Telephony	Peer-to-Peer File Sharing
Streaming Media	

SECURITY RISK:

Bot Networks	Hacking
Instant Messaging	Keyloggers
Malicious Websites	Phishing and Other Frauds
Potentially Unwanted Software	Proxy Avoidance
Spyware	URL Translation Sites

ENFORCEMENT

Users attempting to circumvent this policy may be subject to disciplinary action, up to and including termination of employment.

REVISION HISTORY

1/1/08
5/15/08
7/1/08

VI. Removable Media Policy

PURPOSE: This policy is meant to minimize the City of Berkeley's exposure to risks associated with removable media, such as malware infections and the loss and/or theft of sensitive information.

City employees are permitted to use only removable media that adheres to Department of Information Technology removable media standards published on iCoBWEB/helpdesk and is owned by the City of Berkeley. Privately owned removable media is prohibited from use on City of Berkeley network resources. When information is stored on removable media, it must be encrypted in accordance with the City of Berkeley's Encryption Policy.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

TERMS AND DEFINITIONS

Removable Media: A device or disk that is readable and/or writeable and is able to be moved from computer to computer without modification to the computers. Examples include flash memory devices (such as thumb drives, cameras, MP3 players and PDAs), removable hard drives (and hard drive-based MP3 players), optical disks (such as CDs and DVDs), and floppy disks.

Encryption: A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Sensitive Information: Information which, if made available to unauthorized persons, may adversely affect the City of Berkeley, its programs, or participants served by its programs.

Malware: Software of malicious intent and potential impact

REVISION HISTORY

1/1/08
5/15/08

VII. Physical Security Policy

PURPOSE: To establish standards for physical safeguards to protect against theft of or unauthorized access to City Computer Network Resources.

- This policy takes into account the fact that the physical security requirements of various City of Berkeley facilities are not entirely consistent. They vary depending on the type of equipment deployed, the sensitivity of the data in use, as well as the physical layout of the facility. Accordingly, the physical security measures implemented throughout the City are tailored to the unique requirements of each facility. These measures include restricted security zones, locked doors, access control systems, intrusion alarm systems, approved security containers and destruction equipment.
- Precautions specific to the Data Centers: Due to the especially critical role of the City's two Data Centers (one in the Civic Center and the other in the Public Safety Building), those locations are protected by locks, fire suppression systems, and air conditioning units sufficient to maintain temperatures between 68 and 74 degrees Fahrenheit.
- Precautions specific to remote network equipment: Routers, switches, servers, and other network equipment at locations other than one of the Data Centers are secured within enclosures (e.g., closets or cabinets) accessible only to DoIT. All such enclosures provide ventilation sufficient to meet OEM specifications.

NOTE: Telephony equipment enclosures shall be accessible to both DoIT staff and authorized Public Works Department personnel.

- Precautions specific to workstations: Measures related to the physical security of individual workstations are largely entrusted to users. In this regard, the best practices that are conveyed to users (via Core IT Training, Everyone Emails, etc.) include:
  - Not sharing login credentials (and not enabling others to work under the auspices of one's login credentials)
  - Not leaving an unlocked desktop
  - Saving data on the City network, NOT on the workstation's hard drive
  - Locking doors and windows when leaving work
  - Reporting thefts of computers and related equipment promptly to the Berkeley Police Department and to DoIT
  - Using only approved wireless devices that can be "locked" or "wiped out" from a central location

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REVISION HISTORY

1/1/08
5/15/08

VIII. Servers, Routers, & Switches: Configuration & Security Policy

PURPOSE: To establish standards for the configuration and security of servers, routers, and switches owned and/or operated by City of Berkeley.

1. Administrative Responsibilities:

- DoIT technicians function as administrators for all of the City of Berkeley's servers, routers, and switches. In some cases, limited aspects of application server administration may be shared with departmental "power users" and/or vendors. However, configuration and maintenance of server hardware and operating systems are strictly the responsibility of DoIT technicians.
- All servers, routers, and switches must be included in DoIT's inventory. At a minimum, the following information must be recorded:
  - Server name, serial number and location
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Server configuration changes must follow DoIT change management procedures.

2. General Configuration Guidelines:

- Operating System configuration should be in accordance with approved DoIT guidelines
- Services and applications that will not be used must be disabled where practical
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function
- Do not use root-level access when a non-privileged account will do
- Privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment
- Servers are specifically prohibited from operating from uncontrolled cubicle areas

3. Monitoring:

- All security-related events on production systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week
  - Daily incremental tape backups will be retained for at least 1 month
  - Weekly full tape backups of logs will be retained for at least 1 month
  - Monthly full backups will be retained for a minimum of 1 year

- Security-related events will be reported to the DoIT Security Officer for investigation and follow-up. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host
- Compliance:
    - Server logs and maintenance records will be audited regularly in accordance with the Logging for Audits Policy.
    - Anomalous audit results will be reported, as appropriate, to IT Management, to the DoIT Security Officer, and/or to the administrator(s) involved
    - Anomalous audit results will be promptly justified or corrected by the applicable administrator(s). Documentation of the justification or correction shall be retained per the Logging for Audits Policy.
    - Every effort will be made to prevent audits from causing operational failures or disruptions

RULES SPECIFIC TO ROUTERS & SWITCHES

- No local user accounts shall be configured on routers. Routers must use TACACS+ for all user authentications.
- The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current enterprise-standard production router password.
- Disallow the following:
    - IP directed broadcasts
    - Incoming packets sourced with invalid addresses such as RFC1918 address
    - TCP small services
    - UDP small services
    - All source routing
    - All web services running on router
- Use enterprise-standardized SNMP community strings
- Access rules are to be added as business needs arise
- The router must be included in the DoIT inventory
- Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REVISION HISTORY

1/1/08
5/15/08
7/25/08

IX. Encryption Policy

PURPOSE: To provide guidance that limits the use of encryption to proven algorithms, and to provide direction to ensure that applicable government regulations are followed.

Data sent outside the City network and to City backup systems must be appropriately encrypted. Authorized communication of confidential data to outside entities and routine storage of confidential data (e.g., Patient Information, Criminal Records, etc.) must be appropriately encrypted.

The use of proprietary encryption algorithms is strictly forbidden unless explicitly approved via written service request by the Director of Information Technology, on a case-by-case basis. Questions about acceptable encryption technologies should be directed to the DoIT Help Desk at 981-6525.

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA are used by qualified Department of Information Technology staff members to establish City of Berkeley encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 256 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. The City of Berkeley's key length requirements will be reviewed at least annually and upgraded as technology permits.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

TERMS AND DEFINITIONS

Proprietary Encryption: An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem: A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

REVISION HISTORY

1/1/08
5/15/08

X. Wireless Communication Policy

PURPOSE: To help secure and protect City information assets by specifying technical requirements for wireless infrastructure and endpoint devices.

This standard specifies the technical requirements that wireless devices must satisfy to connect to a City of Berkeley network. Only those wireless infrastructure devices (e.g., WAPs) and only those wireless endpoint devices (e.g., laptops) that meet the requirements specified in this standard or are granted an exception by the Director of Information Technology via written service request are approved for connectivity to a City of Berkeley network.

All employees, contractors, consultants, and other employees at the City of Berkeley, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the City of Berkeley, must adhere to this standard. This standard applies to all wireless infrastructure devices that connect to a City of Berkeley network or reside on a City of Berkeley site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, "Bluetooth" devices, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

GENERAL REQUIREMENTS

All wireless infrastructure devices that connect to a City of Berkeley network or provide access to City of Berkeley confidential information must:

- Be installed, supported, and maintained by an approved support team
- Maintain a hardware address (MAC address) that can be registered and tracked
- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits
- Not interfere with wireless access deployments maintained by other support organizations

LAB AND ISOLATED WIRELESS DEVICE REQUIREMENTS

All laboratory wireless devices that provide access to City of Berkeley confidential information must conform to the General Requirements (above). Lab and isolated wireless devices that do not provide general network connectivity to the City of Berkeley network must:

- Be isolated from the enterprise network (that is it must not provide any enterprise connectivity) and comply with the Laboratory Security Policy or the DMZ Equipment Policy (as applicable)
- Use Service Set Identifiers (SSID) that differ from City of Berkeley production device SSIDs
- Disable broadcasts of lab device SSIDs
- Not interfere with wireless access deployments maintained by other support organizations

"BLUETOOTH" DEVICE REQUIREMENTS

- All Bluetooth devices must meet v2.1 specifications (unless an exception is authorized in writing by the Network Security Officer).
- Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.
- All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
- If your device allows the usage of long PINs, you must use either a 13 alphabetic PIN or a 19 digit PIN (or longer).
- Switch the Bluetooth device to use the hidden mode, and activate Bluetooth only when it is needed.
- Update the device's firmware when a new version is available.
- Bluetooth units are not to be paired to phones, laptops, etc. while in a public area. If Bluetooth-enabled equipment prompts for a pin after initial pairing, **the pairing request must be refused** and the incident must be reported to DoIT immediately.
- It is the Bluetooth user's responsibility to comply with this policy.
- Bluetooth users must only access City of Berkeley information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to DoIT.
- DoIT shall perform audits to ensure compliancy with this policy. In the process of performing such audits, DoIT shall not eavesdrop on any phone conversation.
- The following is a list of unauthorized uses of City of Berkeley-owned Bluetooth devices:
  - Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
  - Using City of Berkeley-owned Bluetooth equipment on non-City of Berkeley-owned Bluetooth enabled devices.
  - Unauthorized modification of Bluetooth devices for any purpose.

HOME WIRELESS DEVICE REQUIREMENTS

All home wireless infrastructure devices that provide direct access to a City of Berkeley network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the City of Berkeley internal network. Access to the City of Berkeley internal network through this device must use standard remote access authentication.

ENFORCEMENT

Any employee found to have violated the policy may be subject to disciplinary action, up to and including termination of employment. Any violation of the policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the City of Berkeley.

TERMS AND DEFINITIONS

AES: Advanced Encryption System

City of Berkeley Network: A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services

Enterprise Connectivity: A connection that provides access to a City of Berkeley network

EAP-FAST: Extensible Authentication Protocol-Fast Authentication via Secure Tunneling: authentication protocol for wireless networks

EAP-TLS: Extensible Authentication Protocol-Translation Layer Security, used to create a secured connection for 802.1X by pre-installing a digital certificate on the client computer

Enterprise Class Teleworker (ECT): An end-to-end hardware VPN solution for teleworker access to the City of Berkeley network

Information Assets: Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization

MAC Address: The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network

PEAP: Protected Extensible Authentication Protocol, a protocol used for transmitting authentication data, including passwords, over 802.11 wireless networks

Service Set Identifier (SSID): A set of characters that give a unique name to a wireless local area network

TKIP: Temporal Key Integrity Protocol, an encryption key that's part of WPA

WPA-PSK: WiFi Protected Access pre-shared key

REVISION HISTORY

1/1/08
5/15/08
6/30/08

XI. Logging and Scanning Policy

PURPOSE: To codify procedures for electronic security scanning of the City of Berkeley's network, and to ensure that all information systems that are subject to audits shall record and retain appropriate log information.

LOGS ARE MAINTAINED TO ANSWER THE FOLLOWING QUESTIONS:

1. What activity was performed?
2. Who or what performed the activity, including where or on what system the activity was performed from (subject)?
3. What the activity was performed on (object)?
4. When was the activity performed?
5. What tool(s) was the activity was performed with?
6. What was the status (such as success vs. failure), outcome, or result of the activity?

SCANS MAY BE CONDUCTED IN ORDER TO:

1. Ensure integrity, confidentiality and availability of information and resources
2. Investigate possible security incidents to ensure conformance to City of Berkeley security policies
3. Monitor user or system activity where appropriate

LOGGING

For the systems covered by this policy, logs shall be created whenever any of the activities listed below is performed or attempted:

1. Data access:
   - Creation of, reading, updating, or deletion of confidential information, including confidential authentication information such as passwords
   - Creation of, reading, updating, or deletion of information not covered in #1
2. Network access:
   - Initiation of a network connection
   - Acceptance of a network connection
   - User authentication and authorization for activities covered in #1 or #2 such as user login and logout
3. Modifying permissions and configurations:
   - Granting, modifying, or revoking access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes
   - System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
4. Application events:
   - Application process startup, shutdown, or restart
   - Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault

5. Suspicious events:
    - Detection of suspicious/malicious activity from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, anti-spyware system, etc.

LOG CONTENTS AND RETENTION

1. Logs identify or contain at least the following elements:
    - Type of action: examples include authorize, create, read, update, delete, and accept network connection
    - Subsystem performing the action: examples include process or transaction name, process or transaction identifier
    - Identifiers (as many as available) for the subject requesting the action: examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
    - Identifiers (as many as available) for the object the action was performed on: examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
    - Before and after values when action involves updating a data element, if feasible
    - Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time
    - Whether the action was allowed or denied by access-control mechanisms
    - Description and/or reason: codes of why the action was denied by the access-control mechanism, if applicable
2. Log Formatting and Storage:
   The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting:
    - Microsoft Windows Event Logs collected by a centralized log management system;
    - Logs in a well documented format sent via syslog, syslog-ng, or syslogreliable network protocols to a centralized log management system;
    - Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and
    - Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

SCANNING

Electronic security scanning of the City of Berkeley's network will be performed under one of two circumstances:

- When such a scan is appropriate to a particular security investigation
- For the purpose of performing routine periodic audits

Security investigations are undertaken in response to either an alert from internal DoIT monitoring systems, a request by the City Manager, and/or Department Directors (with City Manager approval).

ROUTINE PERIODIC AUDITS

Routine scanning includes, but is not limited to:

1. Microsoft Windows Systems
   - Five servers, chosen randomly from the core technologies pool
   - Run vulnerability scan (MBSA) using up-to-date signatures
   - Examine boot files, logs and key permissions for evidence of compromise
   - Validate all running services as correct and appropriate
   - Document findings
2. Firewalls and Routers
   - Both City of Berkeley network firewalls
   - One router and one switch selected randomly
   - Ensure that all systems run the most secure General Deployment IOS versions
   - Verify ACLs, conduits, IP inspects and fixes for configuration errors
   - Examine current configurations for appropriate access levels
   - Validate changes to the Network Topology Diagram (< not a real link); identify potential ingress points
   - Document findings
3. Wireless Vulnerability
   - Discover all wireless access points (WAPs) with City of Berkeley facilities that are accessible outside of those facilities
   - Gather security configurations from the WAPs, and attempt to exploit them in order to access the City of Berkeley's network
4. Internet Vulnerability
   - Perform external scan of the City of Berkeley's connection to the Internet.
   - Document all open ports found and protocol vulnerabilities in those open ports

WORK PERFORMED BY OUTSIDE VENDORS & CONTRACTORS

To enable outside auditing, IT Management shall do the following:

- Authorize the creation of temporary user accounts (with necessary privileges, in accordance with the Network Access Policy) for the individuals who will be performing the scans
- Indemnify (in writing) the contractor against service degradation and/or interruption stemming from the scanning, unless due to the contractor's gross negligence or intentional misconduct
- Identify (in writing) for the contractor an internal contact person to be available if the contractor has questions or requires assistance
- Agree (in writing) with the contractor on specific dates and times for the scanning to occur

ENFORCEMENT

Users attempting to circumvent the log and/or data collection efforts covered by this policy may be subject to disciplinary action, up to and including termination of employment.

REVISION HISTORY

1/1/08
5/15/08
6/30/08

XII. Disaster Recovery Policy

The Department of Information Technology (DoIT) Disaster Recovery Policy is currently being updated, to be finalized no later than **11/30/08.** When complete, the updated policy will be added to the online version of this Master Plan at: **http://icobweb/ITMasterPlan.asp**.

Strategic Technology Initiatives FY09-FY11: Staff Leadership

	IT Project Manager	IT Resource (* = Vendor)	Dept. Project Manager	Department
Community Access				
1. Interactive Voice Response (IVR)	K. Skinner	J. Koontz	R. Eichorn	CMO
2. Expanded Online Services	K. Skinner	E. Yang N. Mehta K. Plante	R. Eichorn	CMO
3. Public Access Computer Labs	S. Sabatino	D.Westmoreland	A. Abramson R. Lowe S. Ferris	Library HHS Parks
4. Community Relationship Management (CRM)	K. Skinner	E. Yang	R. Eichorn	CMO
Enterprise Business Applications				
5. Middleware	B. Thorman	E. Yang	N/A	IT
6. ECM: Enterprise Content Management	K. Skinner	J. Ferguson	D. Despain	Clerk
7. EPM: Enterprise Project Management	E. Yang		T. Vesely	CMO
8. Financial Management (FUND$)	K. Skinner	A. Soussa		Finance
Departmental Work Group Applications				
9. Fire Alpine System	M. Gilbert	*	J. Conti	Fire
10. Police New World System	M. Gilbert	*	A. Greenwood	Police & Fire
11. HHS: PHPIMS	R. Lowe	N. Mehta E. Yang	J. Berreman	HHS
12. Public Works Transfer Station System	C. Delgado	*	P. Holtzclaw	Public Works
13. Public Works Asset & Infrastructure	C. Delgado	*	A. Clough	Public Works
14. Finance Business Licenses			H. Murphy	Finance
15. Finance Grants Management	K. Skinner		M. Tam	Finance
16. Planning Land Use	B. Lavin	J. Koontz	D. Sanderson	Planning
17. Planning Toxics Management System	B. Lavin	J. Koontz	D. Sanderson	Planning
18. Housing Management System				Housing
19. Auditor Electronic Timecards	E.Rodriguez	A. Soussa	B. Zandipour	Payroll
20. Rent Board Records Management System	K. Skinner	J. Ferguson	D. Jojola	Rent Board
21. PR&W Marina Management System				Parks
22. PR&W Online Reservation System	K. Skinner	*	R. Miller	Parks
Data Warehousing & Analysis				
23. Data Warehousing	E.Rodriguez	I. Lapidus	N/A	IT
24. Enterprise Reporting & Analysis	E.Rodriguez	B. Quinn	N/A	CMO
25. Geographic Information Systems (GIS)	B. Quinn	C. Delgado	N/A	IT
26. Youth Data Project			AGallegos-Castillo	CMO
Organizational Development				
27. Online Training System	S. Sabatino	N. Stubbs	L. Schiff	HR
28. Core IT Training	S. Sabatino	*	N/A	IT
29. Hiring, Intake, & Testing	B. Thorman	*	K. Whitfield	HR
Network Operations				
30. Network Security	S. Sabatino	A. Munoz	N/A	IT
31. Green IT	S. Sabatino	B. McGrath	N/A	IT
32. Wireless Field Operations	B. Jennings	E. Yamada	N/A	IT
33. Voice/Internet Protocol (VoIP)	B. Jennings	E. Yamada	N/A	IT
34. Disaster Recovery	B. Jennings	B. McGrath	N/A	IT
35. Standardized Desktops	S. Sabatino	D.Westmoreland	N/A	IT

Note: Cells filled with yellow shading indicate resources not yet identified / assigned.

Strategic Technology Initiatives FY09-FY11: Estimated Staff Costs

	TGG Priority	Estimated Technical Staff (Months)	Departmental Commitment (FTE)
1. Interactive Voice Response (IVR)	1	10	.2
2. Expanded Online Services	1	12	.1
3. Public Access Computer Labs	3	6	.25
4. Community Relationship Management (CRM)	1	24	.3
5. Middleware	1	24	N/A
6. ECM: Enterprise Content Management	2	12	.5
7. EPM: Enterprise Project Management	3	12	.25
8. Financial Management (FUND$)	2	72 (36x2)	.75
9. Fire Alpine System	1	6	.3
10. Police New World System	1	N/A	.5
11. HHS: PHPIMS	2	24	1.0
12. Public Works Transfer Station System	1	12	.2
13. Public Works Asset & Infrastructure	2	18	.2
14. Finance Business Licenses	3	12	.3
15. Finance Grants Management	2	6	.2
16. Planning Land Use	3	24	.5
17. Planning Toxics Management System	1	12	.2
18. Housing Management System	3	10	.5
19. Auditor Electronic Timecards	3	18	.3
20. Rent Board Records Management System	2	18	.3
21. PR&W Marina Management System	2	18	.25
22. PR&W Online Reservation System	1	12	
23. Data Warehousing	2	18	N/A
24. Enterprise Reporting & Analysis	2	6	.2
25. Geographic Information Systems (GIS)	1	6	N/A
26. Youth Data Project	3	TBD	TBD
27. Online Training System	3	6	.3
28. Core IT Training	1	3	N/A
29. Hiring, Intake, & Testing	1	6	.3
30. Network Security	1	18	N/A
31. Green IT	1	18	N/A
32. Wireless Field Operations	2	6	N/A
33. Voice/Internet Protocol (VoIP)	2	12	N/A
34. Disaster Recovery	1	6	
35. Standardized Desktops	1	12	

Note: Cells filled with yellow shading indicate resources not yet identified / assigned.

Strategic Technology Initiatives FY09-FY11: Estimated Timelines

	FY09				FY10				FY11			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Community Access												
1. Interactive Voice Response (IVR)												
2. Expanded Online Services												
3. Public Access Computer Labs												
4. Community Relationship Management												
Enterprise Business Applications												
5. Middleware												
6. Enterprise Content Management												
7. Enterprise Project Management												
8. Financial Management (FUND$)												
Departmental Work Group Applications												
9. Fire Alpine System												
10. Police New World Systems												
11. HHS: PHPIMS												
12. Public Works Transfer Station												
13. Public Works Asset & Infrastructure												
14. Finance Business Licenses												
15. Finance Grants Management												
16. Planning Land Use												
17. Planning Toxics Mgmt System												
18. Housing Management System												
19. Auditor Electronic Timecards												
20. Rent Board Records Mgmt System												
21. PR&W Marina Mgmt System												
22. PR&W Online Reservation System												
Data Warehousing & Analysis												
23. Data Warehousing												
24. Enterprise Reporting & Analysis												
25. Geographic Information Systems												
26. Youth Data Project												
Organizational Development												
27. Online Training System												
28. Core IT Training												
29. Hiring, Intake, & Testing												
Network Operations												
30. Network Security												
31. Green IT												
32. Wireless Field Operations												
33. Voice/Internet Protocol (VoIP)												
34. Disaster Recovery												
35. Standardized Desktops												

Community Access

Strategy: *Upgrade the public computer lab, web, and telephone infrastructure.*

Technology is a powerful tool for facilitating community access to municipal information and services. In recent years, e-agendas, streaming video, email subscriptions, records online, and other web tools at www.CityOfBerkeley.info have improved the convenience and efficiency with which residents, businesses, and visitors connect to the City of Berkeley.

A scaleable infrastructure that enables non-traditional access to City services is critical to keeping e-Government efforts moving forward. Implementing technical 'building blocks' that all departments can leverage to offer expanded web and telephone services to the public is key. Well-maintained computer centers that enable all community members' access to the Internet is also a critical component of the City's Community Access

Berkeley's 125th Anniversary Community Photo

Goal

A technology infrastructure that helps residents, businesses, and visitors access City information and services in a manner that is efficient and convenient, includes 24x7x365 access via web and telephone, and reflects Berkeley's commitment to helping community members on all sides of the digital divide.

Community Access: Key FY09-11 Strategic Initiatives

1. Interactive Voice Response (IVR)

Enable self-service by automating interactions with the City's back-end computer systems and making them available via telephone 24x7. In addition, IVR provides staff with call statistics to assist in resource allocation.

2. Expanded Online Services

Broaden the functionality of the City's current online service center at www.CityOfBerkeley.info/onlineservice to serve as 'one-stop shop' for the most frequently requested services in all departments.

3. Public Access Computer Labs

Centralize support and maintenance of the City's public **computer labs** at recreation centers and senior centers that were 'state-of-the-art' when opened, but currently in varying states of disrepair.

4. CRM

Integrate Community Relationship Management (CRM) software with back-end systems to permit service request intake, tracking, resolution, and reporting from a single, customer-centric interface available to staff at City offices and community members via Internet and telephone.

1. Interactive Voice Response (IVR)

Project Manager: Keith Skinner, 981-6551

Interactive Voice Response (IVR) will enable self-service both during and after regular business hours by providing 24x7 access to City information and services. By automating routine, customer-centric business processes, IVR will not only increase community satisfaction, but also improve efficiency throughout the City's customer service program.

IVR retrieves information from the City's back-end computer systems based on requests entered or spoken by the caller. It can also be used to help filter inbound call traffic to smooth peaks and troughs across call center queues, thus adding a degree of predictability to call volume modeling and staffing. In addition to the most basic benefits of IVR, it also addresses the increasing popularity of self-service and 24x7 access, where community members obtain the service they need when they need it.

Top Business Drivers

1. Community demand for 24x7x365 access to routine City information and services.
2. City council directive to reduce 'call transfers' and 'wait times' for customer service calls.
3. Limited resources for staffing call centers throughout the City.

FY 2009-2011 Action Items

- Finalize technical protocol for connecting IVR system to City's back-end systems by **8/30/08.**
- Prioritize 311 services for IVR-enablement by **9/15/08.**
- Implement Pilot IVR System for Building Inspections in Planning Department by **12/31/08**.
- Identify & implement Pilot IVR project for 311 Call Center by **3/31/09**.
- Conduct community focus surveys on IVR user-friendliness and effectiveness by **4/30/09**.
- Develop implementation plan & schedule for IVR rollout to all departments by **6/30/09**.

Target Outcomes & Measurement

1. 50% decrease in calls with wait times over 5 minutes.
2. 75% decrease in call transfers.
3. 80% Community survey rating IVR system and menus as "good" or "excellent".

2. Expanded Online Services: Online Service Center

Project Manager: Keith Skinner, 981-6551

The Online Service Center is meant to serve as a "one-stop" web portal for 70-80% of all customer service inquiries, no matter which department handles the associated service delivery. Maintained by the 311 Customer Service Center, the Online Service Center provides streamlined access to routine City information and services by connecting web visitors directly to back-end computing systems so that they can submit a service request, check on the progress of a previously submitted service request, pay City fees, and download information.

www.CityOfBerkeley/onlineservice

Top Business Drivers

1. Community demand for 24x7x365 access to routine City information and services.
2. Implement online self-service options to improve community satisfaction.
3. Fiscal pressures to increase the efficiency of Citywide customer service.

FY 2009-2011 Action Items

- Appoint online service center web coordinator in customer service division by **8/30/08.**
- Implement middleware to allow online access to City's back-end computer systems by **8/30/08.**
- Implement online service and staff directories by **10/30/08.**
- Implement online Parks Reservation system by **10/30/08.**
- Implement online payment engine by **12/31/08.**
- Collect and analyze feedback regarding online service center performance by **1/30/09.**
- Offer business license renewal via online service center by **6/30/09.**
- Online permit application and payment by **3/31/10.**
- Identify, develop, and deploy additional City services by **6/30/10.**

Target Outcomes & Measurement

1. 100% participation of all City Departments in populating online service center menus**.**
2. 50% increase in visits to the online service center**.**
3. 20% of all parking and recreation fees paid via online service center**.**
4. 75% Community survey rating online service center "good" or "excellent"**.**

3. Public Access Computer Labs

Project Manager: Sue Sabatino, 981-6553

Public Access Computer Labs expand access to information technology, provide learning services, and support after-school, workforce development, recreation, seniors, and library programs. Although 'state-of-the-art' when opened, these labs are in need of upgrades, ongoing maintenance, and expanded educational programs that leverage partnerships between City Departments, the Berkeley Public Library, and local community organizations to address the digital divide by offering computer resources and training. Public Access Computers are located at:

- Library Central Branch - 2090 Kittredge Avenue
- Library Claremont Branch - 2940 Benvenue Avenue
- Library North Branch - 1170 The Alameda
- Library South Branch - 1901 Russell Street
- Library West Branch - 1125 University Avenue
- Martin Luther King Youth Services Center - 1730 Oregon Street Berkeley
- Frances Albrier Community Center - 2800 Park Street
- Live Oak Community Center - 1301 Shattuck Avenue
- James Kenney Community Center - 1720 8th Street
- Willard Clubhouse - 2720 Hillegass Avenue
- North Berkeley Senior Center – 1901 Hearst Avenue
- South Berkeley Senior Center – 2939 Ellis Street
- West Berkeley Senior Center – 1900 Sixth Street

Top Business Drivers

1. Community demand for neighborhood-based Internet access and computer literacy instruction.
2. City Council commitment to addressing the digital divide.
3. Aging equipment in need of upgrades and maintenance.

FY 2008-2010 Action Items

- Submit digital divide grant application by **12/31/08.**
- Develop Coordinated Community Computer Lab Support Plan by **7/30/09.**
- Develop a standard kiosk configuration by **10/31/09.**
- Standardize Desktop Image at all labs by **12/31/09.**
- Implement Maintenance & Replacement Schedule & Staffing by **1/31/10.**

Target Outcomes & Measurement

1. 50% increase in "uptime" availability of computers in public access labs (to 99.999%).
2. Community feedback surveys rating 90% of all computer labs "good" or "excellent".

4. Community Relationship Management (CRM)

Project Manager: Keith Skinner, 981-6551

CRM (**C**ommunity **R**elationship **M**anagement) software tracks which interdepartmental City services a community member has requested, the delivery dates associated with each service, and billing information associated with the community member's property or service. The information is centralized (rather than stored ***departmentally***) to provide direct access to management, line staff, community members themselves, and other systems (such as IVR and WCM) that might send information to and receive updates from the CRM system. In addition, CRM systems guide customer service representatives through routine service calls to ensure consistent and accurate information and service delivery protocols.

311 Customer Service Team

Top Business Drivers

1. City Council directive for more consistent and effective customer service.
2. Fiscal pressure to improve customer service efficiency.
3. Organizational need to integrate service delivery across departmental areas.

FY 2008-2010 Action Items

- "Soft launch" internal use of CRM software in 311 customer service center by **8/30/08.**
- Integration of CRM with back end system for all refuse billing services by **12/31/08.**
- "Soft launch" of 311 service by **1/30/09.**
- "Soft launch" of online public portal by **3/1/09.**
- Integration of IVR and online payment gateway with CRM by **5/1/09.**
- Expansion to additional operational units by **6/30/10.**

Target Outcomes & Measurement

1. Integration of CRM with operational backend systems.
2. 60% decrease in requests for service directly from operational departments.
3. 75-85% first call resolution in the 311 center**.**

Business Applications

Strategy: *Implement a service oriented architecture (SOA) for software interoperability and scalability.*

Major software applications at the City of Berkeley fall into two categories: **Enterprise Applications** that all Departments depend upon and **Departmental Applications** that one or a few City departments use to guide specific business processes. Traditionally, the relationship across enterprise applications, as well as between enterprise and departmental applications, has been inconsistent due to incompatible software selection. In FY09-FY11, DoIT will implement a centralized framework for software development based on 'Services Oriented Architecture' (SOA) principles to maximize interoperability, save development costs, and expedite development cycles.

Business Applications Team

SOA facilitates the flow of information from one software package to another. Normally, the flow of information to support a simple customer request, such as fixing a pothole, can be quite complex as it crosses different departments, service desks, and software systems to reach the work crews who ultimately complete the work. SOA succeeds by facilitating software integration through the re-use of logic (or 'services'). By reusing the same services in different software packages, programmers can build-in the hooks necessary to connect one software package to another. Each of the projects in the City of Berkeley's FY09-FY11 applications development portfolio will employ SOA to maximize both integration across City software packages and return on our technology investments.

Goal

A Service Oriented Architecture (SOA) that governs all software investments utilizing sound business analysis principles and maximizing interconnectivity across business applications via a library of centralized, reusable logic.

Key FY09-11 Strategic Initiatives: Enterprise Business Applications

5. Middleware

Central to the City's planned Service Oriented Architecture for business applications, middleware will provide a common technical 'glue' such so that software systems normally unable to communicate with one another can trade information.

6. Enterprise Content Management

In partnership with the Department of the City Clerk, improve and expand workflow, records management, and document management system technologies.

7. Enterprise Project Management

Select and implement an EPM software system to manage, monitor, and assess the status of Citywide projects and special initiatives.

8. (FUND$)

Conduct a needs analysis and produce an implementation plan for replacing the City's core back-end financial system in the next 3-5 years.

Key FY09-11 Strategic Initiatives: Departmental Work Group Applications

9. Fire	Complete the implementation of the **Alpine Fire System** in order to improve fire department records management and integrate appropriate fire department workflows with those of the police department.
10. Police	Complete the implementation of **New World Systems**, which includes computer-aided dispatch, records management, and patrol vehicle remote access modules.
11. HHS	Complete the implementation of the **Public Health Patient Information Management System (PHPIMS).**
12. Public Works	Select and implement a new **Transfer Station Management** system to improve routing of refuse collection trucks, administration of bin inventories, payment, and customer follow-up.
13. Public Works	Select and Implement a new **Asset & Infrastructure Management** system to improve analysis, maintenance, regulatory control, and reporting on City's streets, sewers, and storm drains.
14. Finance	Select and Implement a new **Business Licensing** system to replace the existing HTE module with a "best of breed" product that enables online filing and tracking, and connects more directly to regional and state databases for updated regulatory information.
15. Finance	Select and implement a new **Grant Management** system to improve tracking and oversight of grants throughout all City departments.
16. Planning	Select and implement a new **Land Use** system to ensure adherence to all City regulations, streamline permit and plans processing, and improve overall service delivery to planning department customers.
17. Planning	Implement a hosted **Toxics Management**, system then evaluate the necessity and feasibility of migrating the hosted system to an onsite system.
18. Housing	Select and implement a new **Housing Management** system to administer the City's public housing programs.
19. Auditor	Select and implement a new **Electronic Time Card** system to streamline payroll activities, reduce manual data-entry and paper processes, and provide improved internal controls.
20. Rent Board	Design and implement a **Records Management & Workflow** system to streamline Rent Board operations.

Key FY09-11 Strategic Initiatives: Departmental Work Group Applications

21. Parks

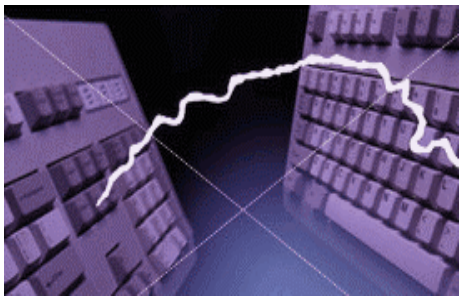
Select and implement a new **Marina Management** system to administer berth assignments and facilitate online payments.

22. Parks

Select and implement a new **Online Reservation and Payment** system for camps and other recreation programs.

5. Middleware

Project Manager: Beth Thorman, 981-6552



Middleware connects two or more separate software applications, allowing them to "speak the same language" and exchange data. As demand for speedier business processing and more efficient data management grows, inter-application integration between software such as core financial system (FUND$), web content management (WCM), geographic information systems (GIS), and community relationship management (CRM) becomes critical. Middleware facilitates such integrations, and assists in improving business process workflows that are currently dependent on separate applications.

Middleware is the core component of the City's Service Oriented Architecture (SOA) because it provides a set of enabling services that maximize interoperability and scalability in all City software. Discreet functions within each application can be packaged as services that can then be combined with other services to provide a complete solution. These services can be used multiple times in multiple ways, affording a great deal of flexibility and scalability. Since useful pieces of legacy software can be combined with new systems, the ROI of each software investment can be increased.

Top Business Drivers

1. Increased demand for integration with legacy applications (such as FUND$).
2. Greater need for integration between independent enterprise and workgroup applications (such as GIS, WCM, and CRM).
3. Inefficient business process workflows involving separate applications.
4. Duplicate sources of the same data in separate applications due to a lack of integration options.

FY 2009-2011 Action Items

- Develop Middleware Platform and Network Architecture by **7/31/08.**
- Pilot integration of FUND$ with Lagan CRM by **8/15/08.**
- Full integration of FUND$ refuse billing processes by **12/31/08.**
- Integrate CRM Application with PW Work Order System by **3/1/09.**
- Develop a Middleware Platform to Support Enterprise Data Warehousing by **12/31/09.**
- Expand integrations to additional operational units by **3/31/10.**

Target Outcomes & Measurement

1. 50% improved efficiency in 311 Call Center workflows (measured via survey of call center agents).
2. 50% reduction in vendor customization costs (by leveraging Middleware instead of point-to-point integrations).

6. ECM: Enterprise Content Management

Project Manager: Keith Skinner, 981-6551

Enterprise Content Management (ECM) is an ongoing and evolving strategy for managing, storing, and delivering public records throughout the City. The City's ECM system includes workflow and business process intelligence systems. Government agencies are legally required to store public documents in a safe and secure manner. In addition, there is an increased public demand for access to public records and information, as well as an internal need for re-use of information within the organization.

Top Business Drivers

1. Legal requirements for records retention.
2. Increased public demand for easier access to information public records via the Internet.

FY 2009-2011 Action Items

- Implement building permits & plans imaging by **12/31/08.**
- Consolidate & upgrade current ECM system by **6/30/10.**
- Upgrade Records Online functionality by **6/30/10.**
- Begin contract process improvement needs analysis by a date to be specified by the Finance department, depending upon staff availability, no later than **6/30/10.**
- Implement contract process improvement by a date to be specified by the Finance department, depending upon staff availability, **6/30/11.**

Target Outcomes & Measurement

1. 100% compliance with records-retention laws for the City's public documents.
2. Improvement in public access to City information and services through the new website and 311 Call Center (measured by survey).
3. Consolidation of internal data sources and improved access to information.
4. Streamlined workflow associated with Citywide contracts.

7. EPM: Enterprise Project Management

Project Manager: Eddie Yang, 981-6556

Enterprise Project Management (EPM) is a combination of software and standards that support projects from inception to completion. Once a program has been designed and approved, staff project managers can use standard project management software to forecast timelines, assign staff and funding resources, track costs, detail project tasks, and provide status reports. Decision makers can view project details, such as budget, staff, and timeline impacts on funding sources and other projects or activities in the City. Templates for specific project types can be created to reduce the amount of time and effort required to define and track project activities, and facilitate information sharing across projects throughout the City.

Top Business Drivers

1. Need for Citywide visibility into program resource allocation, budget, and progress.
2. Fiscal pressure for individual and consolidated view of projects to better manage staffing, funding, timelines, and overall coordination.
3. Improved coordination of cross-departmental resources on all projects, particularly City Council's critical initiatives.

FY 2009-2011 Action Items

- Business analysis complete and implementation proposal submitted by **3/30/10.**
- Installation and configuration of EPM software by **9/30/10.**
- Completion of limited pilot implementation by **1/15/11.**
- Completion of Citywide rollout plan by **2/28/11.**
- Citywide implementation complete by **12/31/11.**
- Develop framework for project manager mentoring program by **5/31/11.**
- Pilot EPM by **6/30/11.**
- Evaluate the success and effectiveness of the EPM pilot test by **8/31/11.**
- Roll-out EPM to candidate departments/divisions by **12/31/11.**

Target Outcomes & Measurement

1. Visibility of all Council critical initial programs and special projects from inception to completion.
2. 30% increase in projects completed on time.
3. 20% increase in projects completed within original budget.
4. Standard methods for program definition, budgeting, and project management.

8. Financial Management (FUND$)

Project Manager: Keith Skinner, 981-6551

The City's core financial and work management system (affectionately known as FUND$) was first purchased in 1990. Since that time, changes in technology have outpaced improvements to the system. Hence, the functionality of many FUND$ modules is less than optimal. Planned upgrades to the City's technology infrastructure discussed throughout this Master Plan, such as middleware, data warehousing, and online payment systems will facilitate migration from specific FUND$ modules to more effective 'best-of-breed' software. Utilizing formal business analysis methodologies, staff from the Department of Finance, the Department of Information Technology, Public Works, and the Budget Office will develop a migration strategy and implement module replacements to better support the City's operational needs and strategic goals.

Top Business Drivers

1. FUND$ design and functionality has not kept pace with the City's operational needs.
2. FUND$ total cost of ownership (TCO) is not commensurate with the benefit it delivers.
3. FUND$ utilizes platforms that are increasingly difficult to support.

FY 2009-2011 Action Items

- Develop, pilot, & implement core FUND$ training program by **12/31/08.**
- Finalize application portfolio, which includes usability rankings for all applications, by **10/30/08**.
- Develop composite application plan for extending the life of the most useful FUND$ functions by **12/31/08.**
- Develop action plan for replacement of least useful FUND$ with a combination of new software or hosted systems (SaaS) by **12/31/08.**
- Develop action plan to complete the replacement of remaining FUND$ software by 2012 by **9/1/09**.

Target Outcomes & Measurement

1. Better alignment of financial software with business needs and strategic goals.
2. Reduced total cost of ownership of GMBA software by 10%.
3. Reduce staff training costs with more intuitive user interfaces.

9. Fire Department: Alpine Systems Software

Project Manager: Mark Gilbert, 981-6528

The City's new public safety technology system (PSTS) will replace aging Fire and Police software applications and ensure integration between them. In FY08, Alpine Systems Software was chosen after a thorough needs analysis that identified specific Fire Department business processes that need enhanced automation. This new software will help improve the Fire Department's records management, emergency medical operations and billing, equipment inventory and maintenance, records management, reporting, fire alarm billing activities, and fire inspection program. Furthermore, the software will be configured to trade information with the core dispatch system slated for implementation as part of the New World Systems project (see Initiative # 11). Additional Fire department computer system improvements include upgraded software for coordinating shift assignments and improved ring down systems in each fire station.

Top Business Drivers

1. A large percentage of ambulance billings could not be collected due to inefficient billing practices.
2. Aging FMIS records management system is outdated and no longer supported by vendor.
3. Current FMIS/FUND$ fire inspection billing process ineffective and staff intensive.
4. Need to automate routine Fire Department administrative activities.

FY 2009-2011 Action Items

- Tele-Staff to Alpine (legacy) integration by **10/31/08.**
- New Alpine Fire Records Management (RMS) system Go-Live by **11/30/08.**
- New Computer Aided Dispatch (CAD) integration with Alpine by **12/31/08.**
- Fire station ring-down system replacement implemented by **12/31/08.**
- Alpine Fire Inspection module to FUND$ integration by **4/30/09.**
- Emergency medical patient support and ambulance billing implemented by **6/30/09.**
- Equipment Inventory and Maintenance modules Go-Live by **8/30/09.**

Target Outcomes & Measurement

1. 15% increase in ambulance revenue.
2. 20% increase in fire inspection billing revenues.
3. 50% decrease in administrative staff time devoted to billing activities.

10. Police Department: New World Systems Software

Project Manager: Mark Gilbert, 981-6528

After a thorough needs analysis of the Police Department's operational activities (including the dispatch center that serves both police and fire), New World Systems software was selected to replace the City's aging public safety technology system (PSTS). As the core component of our upgraded PSTS, the new software suite provides a solid foundation for improved public safety operations. The new system will enable centralized collection of public safety data, better insight into public safety trends, and improved crime-prevention tools. To address increasing demands on field units, an improved wireless infrastructure for data exchange between dispatchers, officers, neighboring jurisdictions, and county databases will be implemented to facilitate the rapid transfer of life-saving information like criminal suspect photos, building floor plans, and surveillance video.

Top Business Drivers

1. Fiscal pressure to decrease officer involved no-suspect reporting, i.e. online citizen police reporting.
2. Increasing need for accurate, up-to-date information in the field and for planning activities.
3. Tactical need for standard emergency communication frequencies across jurisdictions for mutual aid response and disaster recovery planning.
4. Desire for increased GIS integration for more reliable emergency planning and dispatch.

FY 2009-2011 Action Items

- New Computer Aided Dispatch (CAD) & In-Car Mobile modules live by **12/15/08.**
- Develop internal controls & workflows for continuous improvement of public safety data and mapping tools by **2/28/09.**
- New Law Enforcement Records Management (LERMS) module live by **7/22/09.**
- Mobile Field Reporting Module Live by **8/14/09**
- Assess requirements, select, and implement a web-based citizen report submission tool by **8/31/09.**
- New Corrections Management System module live by **10/31/09.**
- Identify steps for improving City GIS systems to enable advanced photographic mapping and measurement in the field by **12/31/09.**

Target Outcomes & Measurement

1. 10% decrease in no suspect reports taken by field officers.
2. 25% decrease in overtime spent on maintenance of public safety systems.
3. 10% decrease in staffing time required for public safety GIS data maintenance.
4. 20% decrease in staff time spent preparing reports.

11. HHS: Public Health Patient Information System

Project Manager: Rebekah Lowe, 981-5117

For years, the Department of Health and Human Services has provided exceptional health care to the community using paper-based patient charts and legacy computer systems. Recent industry and legislative changes have amounted to a mandate for modernized technology systems. HIPAA (Health Insurance Portability and Accountability Act) imposes new security and privacy regulations and an industry-wide shift toward electronic medical record (EMR) creates new technology standards for capturing and securing all patient information. Moreover, most Public Health activities are funded by payments received through medical billing and a variety of grants with reporting guidelines that require software to accommodate rapid changes. Over the next few years, patient information management software systems must be upgraded to ensure effective service delivery.

Top Business Drivers

1. HIPAA requirements for the creation, storage and transmittal of confidential health care information.
2. Electronic billing & claims reconciliation modules needed to streamline processes & improve revenue.
3. Grant funding reporting and compliance requirements that are dynamic & may demand nearly real-time processing of patient & service information.
4. Need for enhanced data collection and analytical capabilities for improved, patient care, streamlined workflow, and rapid identification and assessment of events with significant public health consequences.
5. Health care industry's move to an Electronic Medical Record that makes comprehensive health information available to authorized users, and reduces the need to collect and store paper-based documentation.

FY 2009-2011 Action Items

- Develop project budget & obtain funding by **10/31/08.**
- Complete analysis of current Public Health activities & develop process improvement plan required for system development phase by **12/31/08.**
- Identify, evaluate, and contract with health software vendor by **12/31/08.**
- Complete work with vendor to develop and test software components that meet Public Health patient information system mandates by **12/31/09.**
- Complete modifications based on user feedback & conduct system acceptance testing by **3/31/10.**
- Complete business readiness campaign by **6/30/10.**
- Fully implement new software for Public Health Nursing and Public Health Clinics by **6/30/10.**

Target Outcomes & Measurement

1. 30% increase in reimbursement billing within allowable billing period for patient services.
2. 10% decrease in total cost of service for the average patient.

12. Public Works: Transfer Station System

Project Manager: Cristi Delgado, 981-6545

The City's Solid Waste division generates $28 million a year providing services to approximately 25,000 customers. These services, which are expanding, are managed by a combination of applications in the City's FUND$ financial system (customer service accounts and work orders), scale house software, and custom databases. In all cases, the software is outdated and difficult to use. In addition, these disparate systems do not adequately integrate with each other, resulting in double data entry and numerous paper-based side systems. This has impacted not only operations, but mandatory compliance reporting with State agencies. A 2007 project team comprised of Public Works, Finance, and IT staff identified process improvement opportunities for curbside collection efficiency, routing, revenue collection and tracking, and customer response. Key elements in making these improvements will be replacement of aging legacy systems, better integration of software components, utilization of mobile and GIS technology, and streamlined communication between operational units.

Berkeley Transfer Station
1201 2nd Street

Top Business Drivers

1. Aging legacy software is not scaleable and cannot adequately support expanded services planned by Solid Waste Division.
2. Instability and limited capabilities of scale house software causes reduced operational capacity & frequent outages.
3. Performance metrics and billing information is difficult for staff to access.
4. Suspected lost revenues due to inefficient billing process.

FY 2009-2011 Action Items

- Evaluate proposals and select vendor by **9/30/08.**
- Perform hardware / networking needs analysis to support selected product by **3/31/09.**
- Software implementation completed by **6/30/09.**
- Operations monitoring and assessment completed by **8/30/09.**
- Route optimization and other adjustments to operations by **9/30/09.**

Target Outcomes & Measurement

1. Improved capability to perform accurate revenue analysis & collections activities.
2. 10% reduction in cost of average service delivery.
3. Improved workflow, resulting in improved customer service.
4. Improved capability to comply with State reporting requirements.

13. Public Works: Asset & Infrastructure

Project Manager: Cristi Delgado, 981-6545

The Public Works Department maintains a vast portfolio of public assets: 134 traffic lights, 8,000 street lights, 85,000 refuse containers, 653 miles of streets, 500 miles of sanitary sewers, 78 miles of storm sewers, and 300 miles of walkways. Each asset type has its own maintenance cycles and performance metrics, currently managed using the FUND$ work order module. While FUND$ has accommodated the more basic asset management activities, it cannot adequately track more complex activities such as storm drain management, maintenance forecasting, and geo-referencing assets in the public right of way. This not only results in higher operational costs, but also places the City in danger of failing to meet established State and Federal compliance standards. In 2006, Public Works and Information Technology staff worked together to complete a needs analysis for the City's asset management activities and funding was identified to support the selection and implementation of a new asset management system that will provide better proactive maintenance and, subsequently, an overall reduction in cost.

Top Business Drivers

1. State and Federal laws mandate specific reporting requirements that currently either can't be met or require excessive effort to meet.
2. Inability to properly maintain and/or replace assets in a timely manner, resulting in higher operational & emergency repair costs.
3. Reduction in funding sources and spiraling cost of labor and materials necessitates more advanced forecasting tools; performance metrics.

FY 2009-2011 Action Items

- Issue RFP for new system by **8/31/09.**
- Implement new system by **10/31/10.**

Target Outcomes & Measurement

1. 10% reduction in asset maintenance costs.
2. 20% reduction in emergency repair costs.
3. 70% reduction in staff hours required to prepare mandatory State & Federal compliance reports.
4. Improved capability to assess asset performance when making purchasing decisions.

14. Finance: Business Licenses

Project Manager: To Be Determined

Business licenses account for over $11 million in annual General Fund revenue that is used to fund critical City services. Maintaining accurate and timely information is essential to supporting core activities including revenue collection, license issuance, business improvement districts, and customer service. The FUND$ Business License module is limited in its ability to support these functions. A replacement system with more robust features will better equip staff to identify underreported gross receipts, resolve delinquent accounts, and correctly assign business classifications to assess license fees. The new system will also allow business owners to apply and renew business licenses online and support business-related data to be more easily shared across departments such as Economic Development, Public Safety, and Planning.

Top Business Drivers

1. Fiscal pressure to attain greater compliance and increased business license revenues through improved data accuracy and integration of external data sources.
2. Operational need to improve efficiencies through better alignment of software to workflows.
3. Improve compliance, revenue generation, business monitoring and business development.

FY 2008-2010 Action Items

- Complete business analysis and requirements gathering by **12/31/08**, subject to Finance staff availability.
- Identify, evaluate and select software by **3/30/09.**
- System implementation completed by **9/30/09.**
- Integrate new licensing system with CRM by **11/30/09.**

Target Outcomes & Measurement

1. Increase in accuracy of classifying businesses to assess license fees.
2. 20% increase in business license revenue.
3. 50% decrease in delinquent renewals due to online renewal capabilities.
4. Implementation of online business license renewal process.

15. Finance: Grants Management

Project Manager: Keith Skinner, 981-6551

The City of Berkeley relies upon approximately $30 million in grants. Some departments, like HHS and Housing, rely heavily upon this funding, but other departments such as Police, Planning, and Public Works also employ grants as a funding source. Managing grants is a complicated process. Grant managers currently use a variety of systems to track different components of a grant, including FUND$ codes, spreadsheets, and paper files. Replacing these ad hoc tools with a comprehensive solution will require not only new software designed specifically to support grant manager activities, but also improved grant accounting practices. As a result, this project will require substantial process analysis and training prior to implementation, but it has the potential to greatly improve the City's ability to track, manage, and reapply for grant funding.

Top Business Drivers

1. City is not fully utilizing current grant funding due to the lack of adequate management tools.
2. Inconsistent accounting practices amongst grant managers.
3. Budget reductions may endanger some programs if appropriate grant controls are not implemented.

FY 2009-2011 Action Items

- Full analysis of existing grant accounting practices by **12/1/08.**
- Standardize grant account practices Citywide using existing systems by **6/30/09.**
- Identify, evaluate and select specialized grant management software by **12/31/09.**
- Implement grant management software by **3/15/10.**

Target Outcomes & Measurement

1. Standardization of grant accounting throughout City.
2. 35% increase in reimbursement of grant-funded expenditures.
3. 20% reduction in staff time devoted to grant management.

16. Planning: Land Use

Project Manager: Butch Lavin, 981-7493

The Department of Planning & Development not only enforces the City's Zoning Ordinance through the issuance and monitoring of use permits, but also enforces State codes (such as CEQA) and decisions reached by various city commissions like the Zoning Adjustments Board, Planning Commission, and Landmarks Preservation Commission. Staff has historically tracked information to support these activities using an assortment of databases, spreadsheets, and paper systems. The staff time required to maintain such systems is inefficient. Following a formal needs analysis, a more effective software system will be identified and implemented to manage the use permit process from beginning to end, facilitate quick access to information associated with development projects and legislative decisions, and enable integration with the City's major enterprise systems, such as CRM and GIS.

Top Business Drivers

1. Increasing demand for permit process improvements.
2. Inefficiency, high staff cost and risk of error with current systems.
3. Land Use information is not immediately available to other city systems or to community members.

FY 2009-2011 Action Items

- Finalize system requirements by **4/30/09.**
- Select vendor by **6/30/10.**
- Implementation by **6/30/11.**

Target Outcomes & Measurement

1. Project status, hearing schedule and history of determinations available via Internet to community, staff and officials.
2. Ability to share Land Use data with other City systems such as Building Permits, Business Licenses and Public Safety.
3. 25% reduction in staff cost for administration of development projects.
4. 20% reduction in the project delays due to process inefficiencies.

17. Planning: Toxics Management System

Project Manager: Butch Lavin, 981-7493

The Toxic Management Division (TMD) of Planning is charged with regulating 1300 active and inactive sites, including 400 permitted sites that require toxic material and/or storm water monitoring. The chemical inventory and contamination records TMD maintains are important to other departments, such as Public Works and Fire, as well as the general public. For years, TMD has relied upon a collection of public domain software, Access databases and spreadsheets to manage its operations. The goal of this project is to make toxics information more accessible to those who need it, allow the TMD staff to respond to complaints and events in a more timely manner, and to improve the efficiency of monitoring, enforcement, and billing activities.

Top Business Drivers

1. Duplicate sources of the same data in spreadsheets and ad hoc databases due to a lack of integration options. Difficulty creating a comprehensive view of activities and information
2. Inability to spatially reference data due to lack of GIS implementation.
3. Inability to correlate disparate hazardous materials, storm water, and contamination data that reside in different databases.
4. Inability to share data with other agencies and departments.

FY 2009-2011 Action Items

- Implement a Hosted Solution by **12/31/08.**
- Evaluate hosted solution versus bringing the solution on-site by **12/31/09.**
- If bringing on-site, implement on-site solution by **5/31/10.**

Target Outcomes & Measurement

1. Improved efficiency in project time tracking and reporting.
2. 50% of regulated facilities participating in on-line inventory data submission.
3. 50% reduction in paper based data collection.

18. Housing Management System

Project Manager: To Be Determined

The Housing Department, in pursuit of its mission to preserve and support affordable housing, administers an array of complex programs ranging from housing for homeless disabled persons to monitoring affordable housing compliance for new developments. Most of these programs are administered using a variety of spreadsheets and ad hoc databases. Some of the programs have recently been automated, including Shelter Plus Care and Davis-Bacon contractor compliance. The remaining processes require automation to ensure complete compliance and the best service delivery of housing services. The goal of this project is to identify and implement a complete housing management system that will allow Housing staff to concentrate on their specialties and ease the burden of developing their own program administration tools.

Top Business Drivers

1. Complex compliance and monitoring requirements for low income and affordable housing programs that are difficult to track.
2. Inability to reliably detect properties and landlords involved in more than one program.
3. Liability to City for inadequate enforcement of State and Federal regulations.
4. Loss of revenue.
5. Duplication of efforts among multiple staff maintaining individual spreadsheets and inconsistency of the information between them.

FY 2009-2011 Action Items

- Complete full analysis of Housing needs by **6/30/09.**
- Research, evaluate, and select software system by **12/31/09.**
- Implement new software by **4/30/10.**

Target Outcomes & Measurement

1. 25% increase in compliance with Federal and State regulations.
2. 25% increase in housing revenues due to more effective analysis and enforcement regulations.
3. 50% increase in staff efficiency.
4. Increased transparency of all Housing programs for staff, officials, and the public.

19. Auditor: Electronic Timecards

Project Manager: Ernesto Rodriguez, 981-6546

Every two weeks, payroll clerks throughout the city process over a thousand paper timecards, checking budget codes, hour codes, and authorizations. In some departments, this information is keyed into spreadsheets for further tabulation and cross checking and only then entered into the FUND$ payroll system. While the complexity of tabulating employee time cannot be completely addressed by software, it is possible to improve the process of getting information into the payroll system. New electronic timecard software will facilitate the collection of employee time from a variety of sources, provide review and approval capabilities, and interface with the City's existing payroll system.

Top Business Drivers

1. High cost and other inefficiencies and risk of error in having departmental payroll clerks transfer employee time from paper to the City's payroll system.
2. Inability to take full advantage of existing electronic data collection devices (e.g., biometric clocks).
3. Inefficient, costly process to sign and approve paper timecards.
4. Current time collection cycle requires employees to enter some time before it is worked, resulting in unnecessary corrections (for absences and overtime) after timecards have been entered.

FY 2009-2011 Action Items

- Gather time collection requirements from departments by **9/30/10.**
- Identify, evaluate and select electronic timecard system by **1/31/11.**
- Install and configure software and hardware by **3/31/11.**
- Conclude first departmental pilot by **6/1/11.**
- Citywide implementation by **6/30/11.**

Target Outcomes & Measurement

1. 25% reduction in duration of biweekly time collection lifecycle.
2. 50% reduction in payroll clerk time in verifying/entering employee time.
3. More timely submission of time by employees and easier review for supervisors.

20. Rent Board: Records Management & Workflow System

Project Managers: Keith Skinner, 981-6551 & Darcy Jojola, 981-4919

The Rent Board works to ensure compliance with legal obligations relating to rental housing; and to advance the housing policies of the City with regard to low and fixed income persons, minorities, students, disabled, and the aged. Currently, the Rent Board uses an aged UnixWare system and Informix database engine to support its operations. At over ten years old, this system requires redesign to meet current records management and workflow needs, integrate with enterprise systems such as Community Relationship Management (CRM) and Geographic Information Systems (GIS), and adhere to the data storage and security standards that guide Citywide business applications.

Top Business Drivers

1. Current system is aging and vendor no longer supports platform.
2. Desire to increase system efficiency and usability.
3. Demand for easier and more advanced reporting and data analysis.

FY 2009-2011 Action Items

- Business Analysis Complete by **9/30/08.**
- Packaged Software evaluation complete by **12/30/08.**
- Packaged Software vs. Internal Programming Decision by **1/30/09.**
- Pilot Implementation by **9/30/09.**
- System Implementation by **12/30/09.**

Target Outcomes & Measurement

1. 20% decrease in administrative and staff support costs.
2. System compliance with Citywide technical guidelines and data storage standards.
3. Improved reporting and data analysis tools.
4. Web enabled applications and tracking.

21. Parks, Recreation & Waterfront: Marina Management System

Project Manager: To Be Decided

This space intentionally left blank as a placeholder for the Parks, Recreation, and Waterfront Marina Management System project description.

Top Business Drivers

To Be Determined

FY 2009-2011 Action Items

To Be Determined

Target Outcomes & Measurement

To Be Determined

22. Parks Recreation & Waterfront: Online Reservation System

Project Manager: Keith Skinner, 981-6551

For years, Parks, Recreation, & Waterfront (PR&W) has relied on a DOS-based registration system. Registration was conducted either via mail or in person at one of the recreation counters. In addition to being labor intensive and inefficient, the existing process is also difficult from a customer service perspective. The goal of this project is to implement an online reservation system that will allow the public to register for Berkeley camps via the Internet or telephone. The new software will provide better customer service and management of the program's finances.

Top Business Drivers

1. Current system consumes a great deal of costly staff resources.
2. Public must register via mail or in person, often resulting in lag time before registration is confirmed.
3. Cumbersome and ineffective waitlist management.
4. Financial management is inefficient and error prone.

FY 2009-2011 Action Items

- Implement an online registration system pilot by **11/15/08.**
- Evaluate pilot program by **3/15/09.**
- If pilot is a success, expand to facilities, leagues, and other programs by **12/31/09.**

Target Outcomes & Measurement

1. 60% improvement in customer satisfaction.
2. 50% reduction in staff time required to manage program finances.

Data Management

Strategy: *Create a data-warehouse for data collection, storage, and analysis technologies.*

As the City expands its reliance upon technology systems, managing the data produced and utilized by these systems becomes increasingly important. Previously, disparate business applications demanded separate databases. This led to the proliferation of stand-alone databases throughout departments and across applications that are unable to share information, follow inconsistent security protocols, make Citywide trend analysis extremeley difficult, and cost the City licensing fees, risks, and inefficiencies.

Ernesto Rodriquez
Data Warehousing Coordinator

A **data warehouse** is a 'master database' that centralizes data from a range of different sources so that information can be shared across business processes and comprehensively mined to conduct wide-scale management analysis and reporting. In 2008, the City of Berkeley will begin implementing an enterprise data warehouse in order to simplify the collection, storage, security, and utilization of data across business applications, departments, and reporting tools.

Goal

A robust, cost-effective infrastructure for collecting, storing, securing, and analyzing Citywide operational data as a vital public asset for planning and measuring municipal services.

Data Management: Key FY2008-2010 Strategic Initiatives

23. Data Warehousing

Implement a centralized warehouse that integrates data from various operational systems and applications to enable cross-platform data sharing and comprehensive organizational data storage, security, and mining. Centralizing and rationalizing the City's data in this manner is a critical step to maximizing Citywide operations in the coming years.

24. Enterprise Reporting & Analysis

Provide a variety of decision support tools and information products that will accommodate a wide range of users, skills and needs. Used in conjunction with the City's data warehouse, these tools and products will not optimize use of IT staff but also enable line of business users and decision makers to access and analyze enterprise information in a meaningful way.

25. Geographic Information Systems (GIS)

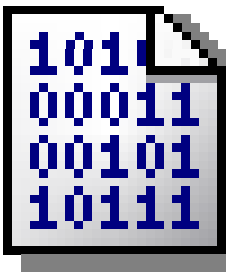
Upgrade the City's Geographic Information Systems (GIS) infrastructure in order to enable integration with core enterprise applications and facilitate more rapid development of spatially oriented analysis tools.

26. Youth Data Project

Proposed project to develop a system whereby the city and Berkeley Unified School District (BUSD) store data and report, via mutually agreed upon outcome measures, on the progress the City of Berkeley is making in overall well-being with children and youth. This data can potentially be used for developing report cards for public consumption.

23. Data Warehousing

Project Manager: Ernesto Rodriguez, 981-6546



A critical issue facing the City of Berkeley is how to most effectively use its vast data stores. Decision-makers - from senior managers to front-line employees - in need of essential business intelligence are increasingly hampered by slow and limited access to data, disparate data sources, format incompatibility, and a lack of historical information. The City's data warehouse is designed to support business decisions by collecting, consolidating, and organizing data to make it more readily available to business applications, reporting tools, and decision-makers.

A data warehouse is a central information repository. Unlike the proprietary data storage platforms that are native to the City's primary legacy systems, a data warehouse stores 'read-only' data that is specifically organized for rapid transfer to a wide variety of business applications and reporting tools. The data-warehousing program will gather and prioritize requirements across City departments and implement a robust data architecture to support the changing needs of users across the City. Priorities for FY08-10 include requirements gathering, data analysis and architecture, system implementation reporting tool selection, staffing, database creation and configuration, data security controls and end-user training.

Top Business Drivers

1. Operational need for centralized, consistent, and accurate information from disparate systems.
2. Fiscal pressure to increase revenue and improves efficiencies via better decision-making.
3. Desire for increased information-driven policy-making.
4. Need for a 'self-service' reporting environment for increased user base without IT interference.
5. Customer-service orientation requires a comprehensive, customer-centric view of data.

FY 2009-2011 Action Items

- Gather Citywide feedback for business needs and prioritization for pilot project by **7/31/08.**
- Identify specific pilot project users and conduct requirements gathering by **7/31/08.**
- Develop a Database Administrator work plan by **10/15/08.**
- Design and implement proof of concept warehouse by **10/30/08.**
- Formalize process for expanding data warehouse to operational units **11/15/08.**
- Establish data governance, security, and meta-data protocols by **12/31/08.**
- Expand data warehouse to operational units **6/30/10.**

Target Outcomes & Measurement

1. Successful gathering of requirements and implementation of pilot reporting project by end of FY08.
2. Development of strategic roadmap for supporting successive data warehouse projects.
3. Implementation of scaleable architecture that can support a range of reporting and analysis needs.
4. Decreased spending on external data subscriptions (e.g. Sales Tax data subscription).
5. Compliance with established data management protocols.
6. Increased number of users and applications using data warehouse information.

24. Enterprise Reporting & Analysis

Project Manager: Ernesto Rodriguez, 981-6546

Improve the use of data in strategic planning & performance measurement. Information is of critical importance to any company. Technology can help empower an organization's most important business asset—your people—by connecting them with the right information quickly, so that they can transform business data into insights and translate insights into organizational knowledge and action. **Reporting** serves as the foundation of a broader business intelligence strategy by **...** reliably and securely—via the web or embedded in **enterprise** applications. By delivering the most-requested information reliably and securely—via the web or embedded in enterprise applications—reports serve as the foundation of a broad business intelligence strategy.

Top Business Drivers

1. Inability to correlate disparate business "facts" that reside in different databases.
2. Need for immediate ad hoc organizational and operational data to inform important decisions.
3. Need for consolidated, simplified view of the city to facilitate policy decisions and monitor performance.

FY 2009-2011 Action Items

- Design and implement proof of concept reporting and analysis service by **10/30/08.**
- Conduct reporting and analytics needs analysis for first operational unit by **1/31/09.**
- Deliver expanded warehouse and analytical tools to first operational unit by **4/15/09.**
- Expand reporting and analysis services to operational units **6/30/10.**

Target Outcomes & Measurement

1. 60% reduction of staff time in obtaining routine information.
2. 70% increase in satisfaction with information available.
3. 45% increase in efficiency of operations due to better monitoring mechanisms.
4. 60% decrease in effort required to assemble ad hoc data for decision-making.
5. 65% reduction in IT service requests for customized reports or data extracts.

25. Geographic Information Systems (GIS)

Project Manager: Brian Quinn, 981-6520

Geographic Information Systems (GIS) provide a spatial view of data. While GIS can be used strictly for generating maps, its most powerful application is as an analytical tool with advanced modeling, forecasting, planning and performance measurement capabilities. The City's GIS program has experienced incremental growth over the past 12 years. While data development efforts have flourished, easy access to the GIS data repository has remained a challenge due to a lack of integration Citywide business processes and enterprise software. Our goal in the coming years is to upgrade the GIS infrastructure to be an easily accessible enterprise tool for data analysis. The new architecture will adhere to the Citywide Service Oriented Architecture (SOA) standards, thereby facilitating more rapid development of GIS applications and enabling a more robust set of web-based GIS services the community via the City's website at www.CityOfBerkeley.info.

Brian Quinn
GIS Coordinator

Top Business Drivers

1. Rapidly changing demand for information to support policy makers and city administration.
2. Governance requiring increasingly complex decision support.
3. Most activities of city government are related to a geographical location.
4. Sophisticated public with increasingly complex information demands.

FY 2009-2011 Action Items

- Redesign and implement physical architecture, including software, by **9/30/08.**
- Fully implement and publish revised policies by **10/30/08.**
- Develop and implement new internal and public GIS web portals by **11/30/08.**
- Complete and deliver "top 10" map services/products for internal use by **12/31/08.**
- Complete and deliver "top 10" map services/products for external use by **4/30/09.**
- Complete and deliver second-generation GIS applications to replace Parcel Popper and Parcel Notifier by **6/30/09.**

Target Outcomes & Measurement

1. Refined, efficient workflow that speeds time to delivery of all products and services.
2. Replacement of existing GIS applications that are difficult to maintain and/or that provide limited functionality.
3. Proliferation of map products and services supporting all areas of business.
4. Self-help portal for both staff and public to optimize use of GIS professionals.

26. Youth Data Project

Project Manager: To Be Determined

The youth data project is to develop a data system whereby the City and Berkeley Unified School District to store data and report, via mutually agreed upon outcome measures, on the progress the City of Berkeley is making in overall well being with children and youth. This data can potentially be used for developing report cards for public consumption. The goal is to provide more robust analytical tools to assess how well children and youth are doing on a variety of levels: education, employment, after-school activities, contact with juvenile justice etcetera.

Top Business Drivers

1. Fiscal and social pressures to maximize efficacy of youth programs throughout the community.
2. Inefficiencies in current data generation and tracking mechanisms.
3. Lack of coordination and performance measurement across City youth programs.

FY 2009-2011 Action Items

- Select Indicators
- Write Tech Requirements
- Identify Technician/Programmer
- Load Data / Test Pilot System
- Desired Go Live

Timelines To Be Determined

Target Outcomes & Measurement

1. Comprehensive overview of youth program monetary investments and key performance measurement metrics.
2. Access to data input and report output by all major youth programs in the City, including those operated by Berkeley Unified School District (BUSD) and community non-profit agencies.
3. Automated quarterly and annual performance reports.

Organizational Development

Strategy: *Promote technology training and purchasing as strategic investments, rather than ad-hoc activities.*

Information technologies are enabling tools and disciplines that assist organizational effectiveness. However, the best technologies will not automatically enable employees to be efficient or effective. Organizational culture - and the degree to which sound planning, business process reengineering, and employee training practices are encouraged - plays an important role in determining whether or not any technology project will succeed.

City of Berkeley Executive Team

Goal

A highly motivated, technically proficient workforce able to utilize the most efficient technologies in delivering excellent City services and coordinate strategic investments across departments, divisions, and business processes.

Workforce Training: Key FY2009-2011 Strategic Initiatives

27. Online Training System

Provide online course development tools that allow subject experts, training professionals and others to develop and deliver specialized training not requiring a classroom setting to be delivered to staff on demand.

28. Core IT Training

Integrate IT training program with Core Course program – in concert with desktop standardization – to include online modules, advanced training in Enterprise Applications, and further training in FUND$, business analysis, and technology project planning.

29. Hiring, Intake, & Testing

Automate hiring and intake procedures for increased efficiency & to support clearly articulated technology skills necessary to gain employment at the City of Berkeley.

27. Online Training System

Project Manager: Sue Sabatino, 981-6553

The City provides a comprehensive classroom-training program for its employees, ranging from core courses such as Conflict Resolution to more specialized safety training for employees who operate heavy equipment. While this classroom training is successful and necessary, there are unmet training needs that could be addressed by focused online training program. For example, online tutorials explaining how to process a purchase requisition or prepare a budget submission could be delivered at the desktop. Supervisors would also be able to require and track compulsory training. Course development tools can be used by business experts, managers, and/or training experts.

Top Business Drivers

1. Increasing demand for Berkeley-specific training and limited staff resources to provide classroom training.
2. Heavy reliance on written or oral communication of specialized policies and procedures.
3. Cost of classroom training not always justified by the level of course material.

FY 2009-2011 Action Items

- Partner with BCM to pilot & publish short online video how-to's by **3/31/09.**
- Identify, evaluate, and select course-authoring software by **3/31/09.**
- Produce prioritized course creation plan by **9/30/10.**
- Publish first series of classes by **11/30/10.**

Target Outcomes & Measurement

1. 25% reduction in cost of classroom training for material that can be disseminated via online training (such as employee orientation).
2. Greater access to training for all staff.

28. Core Information Technology Training

Project Manager: Sue Sabatino, 981-6553

The need for a Core Information Technology Training program has never been greater. Almost one quarter of the 16,000 service requests handled by Help Desk each year involve City employees who need assistance using the core technical tools on their desktops. As we do better job of training City staff to use technology, we can reallocate Information Technology support staff to more complex technical issues, projects, and training for newer technologies. A Core IT Training will also increase overall efficiency in City of Berkeley operations as City employees become more adept at utilizing technology to deliver improved City services.

Top Business Drivers

1. The need to provide Core IT training and policies for new as well as current City of Berkeley staff.
2. To help increase efficiency in City of Berkeley operations by properly utilizing the technology tools given.
3. In providing this training City of Berkeley staff will better understand and use the technology needed to help the City of Berkeley community.
4. By decreasing the number of helpdesk calls IT staff can devote more time to more complex issues, project and newer technologies.
5. To properly explain IT policies regarding security and technology use to all City staff.

FY 2009-2011 Action Items

- Re-analyze data from service request system to determine the most frequently asked questions/problems by **11/30/08.**
- Look at current location of self help documentation to determine if newer documentation is needed by **12/31/08.**
- Develop, pilot, & implement core FUND$ training program by **12/31/08.**
- Modify Core IT training packet to incorporate system upgrades by **1/31/09.**
- Modify Core IT training packet to include Security Best Practices module by **1/31/09.**
- Re-evaluate and expand program as appropriate: **9/30/09 & 9/30/10**

Target Outcomes & Measurement

1. 10% decrease in routine service requests from City of Berkeley staff.
2. 10% increase in iCoBWEB self help visits.

29. Hiring, Intake, & Testing

Project Manager: Beth Thorman, 981-6552

For many years, the Department of Human Resources has coordinated the process of hiring employees with outdated and inefficent technology tools. Most steps in the current process require manual intervention. This cumbersome system is not only inefficient, but also results in lost opportunities with potential hires because the City's hiring process is slower than that of competing organizations. The Human Resources Department's new web-based applicant tracking and intake system will support streamlined hiring processes, from job requisition, to online applications, to employee intake. Hiring managers will be able to request requisitions, review applications and select candidates online. Once a candidate is hired, information will be seamlessly integrated into the payroll system, significantly improving our current intake process. The new applicant tracking system will provide a foundation for further developing online systems for classification-specific testing and tracking.

Top Business Drivers

1. Large number of job openings and applicants overload existing system, resulting in a longer hiring process.
2. Inefficiencies in current system are costly, ineffective and unnecessary.
3. City is losing competitiveness in hiring qualified applicants due to lengthy process.

FY 2009-2011 Action Items

- System configuration and HR staff training by **9/15/08.**
- Departmental staff training by **10/30/08.**
- Internal and external go-live by **11/15/08.**
- Payroll interface implemented by **12/15/08.**

Target Outcomes & Measurement

1. 40% decrease in cost per applicant processing.
2. 20% decrease in average length of hiring process.
3. Ability to better detect and analyze trends and monitor hiring metrics.

Network Operations

Strategy: *Implement updated security tools, consolidate voice and data networks, and launch a Green IT program.*

As City departments, divisions, and business units increasingly implement technical solutions to improve the efficiency of operations, the tasks associated with ensuring efficient network operations, availability, and security become increasingly complex. Adopting industry best practices for converged networks, standardization, security, and disaster recovery will greatly reduce the cost and strain of maintaining the network infrastructure that staff and community members depend upon to conduct their business.

Network Operations Team

Goal

A highly available and fault tolerant network infrastructure that enables City staff to conduct business in a secure, cost-effective, and efficient manner and follows best practices for Green IT.

Network Operations: Key FY08-10 Strategic Initiatives

30. Network Security

Overhaul security protocols and monitoring tools to address new threats and mitigate weak internal controls, including those associated with network access, data protection, and desktops.

31. Green IT

Reduce the City of Berkeley IT carbon footprint by standardization, consolidation, and enforcing green work habits with respect to technology (such as duplex printing).

32. Wireless Field Operations

Enable City staff to access major Enterprise and Departmental applications from the field, to facilitate more efficient service to the community and reduce the need for paper reporting and double data-entry.

33. Voice Over Internet Protocol

Complete a network readiness assessment, mitigation plan, and implementation schedule for consolidating voice and data networks to save costs associated with hardware, licensing, operations, and administration.

34. Disaster Recovery

Comprehensively overhaul disaster recovery and continuity of operations procedures to reflect needs associated with new Enterprise applications, data warehousing, and implementation of Internet-based co-location.

35. Standardized Desktops

Implement standard City desktop and laptop configurations, direct from supplier, with standard application suite to save costs associated with building, maintaining, and deploying disparate machine images.

30. Network Security

Project Manager: Sue Sabatino, 981-6553

It is increasingly common to encounter news that an organization's network has been hacked, Social Security numbers or financial information has been stolen, or missing laptops have led to the loss of mission-critical data. Such security risks are difficult to mitigate in the simplest of network environments. The City of Berkeley's complex business environment and commitment to improved efficiency through expanded technical services make network security an ongoing challenge. For example, increased use of web-based and wireless network access is necessary to increase the efficiency of departmental operations, but inevitably increases network security threats. The Department of Information Technology is committed to mitigating unacceptable security risks throughout all network resources - - including our financial system, police department records, operational databases, Internet connections, servers, desktops, and removable media - - while at the same time equipping City staff with the technology tools they need to deliver excellent community service.

In keeping with security best practices, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Department of Justice (DOJ) regulations, the Department of Information Technology will continue to develop policy recommendations and implement systems that enable regular monitoring, analysis, and correction of behavior on the City's network. Though these restrictions are sometimes difficult to implement, the benefits can lead to not only better security, but also reduced operational costs. For example, standardizing desktops will not only reduce the number of 'back doors' to the network, but also decrease the overall cost of maintaining the City's 1,150 workstations.

Top Business Drivers

1. Growing exposure to potential vulnerabilities and the need to reduce productivity loss.
2. Health Insurance Portability and Accountability Act (HIPAA) and Department of Justice (DOJ) security mandates.
3. Desire to reallocation of IT resources from baseline activities to strategic initiatives.

FY 2009-2011 Action Items

- Implementation of centralized, automated workstation configuration software by **12/31/08.**
- Automated traffic analysis, forensics, patch management, and inventorying by **7/31/09.**
- Implementation of centralized Network Access Control by **12/31/09.**
- Pilot implementation of virtualized desktops by **6/30/10.**

Target Outcomes & Measurement

1. Monthly comprehensive server OS and hardware status reporting**.**
2. Configuration Manager agents verified on 99.999% of City workstations**.**
3. Completion of enterprise asset classification**.**

31. Green IT

Project Manager: Sue Sabatino, 981-6553

By passing Measure G in November 2006, Berkeley voters called for an 80% reduction in community greenhouse gas emissions by 2050 and the development of a Climate Action Plan. Information Technology plays a critical role in supporting this effort. The Environmental Protection Agency reports that energy use in data centers has doubled in the past six years and that, without implementation of Green IT, this trend will continue.

Maintaining an efficient computing infrastructure (including *data centers*, *servers*, *desktops*, *printers*, and *employee work habits*) is one of the most important steps City staff can take to reduce energy consumption, prevent greenhouse gas emissions, and lower the environmental and financial costs of running our municipal government. The City of Berkeley network appliances adhere to EPEAT (Electronic Product Environmental Assessment Tool) criteria. Other programs, such as desktop standardization, E-waste consolidation, and standardized training for Green IT work habits will help support our community commitment to staying green.

Top Business Drivers

1. City Council mandates and Community Commitment to environmental stewardship.
2. Current data center configuration cannot support growth in stand-alone hardware ('server sprawl').
3. Fiscal pressure to reduce hardware, storage, backup, and staffing costs.
4. Legislated mandates for increasingly robust security and disaster recovery.

FY 2009-2011 Action Items

- Baseline IT energy consumption levels by **10/31/08.**
- Standardize "green procurement" for new IT equipment purchases by **6/30/09.**
- Configure and enforce power saver settings for client workstations across the organization by **6/30/09.**
- Implement Consolidated Data Warehouse Server Farm by **8/30/09.**
- Implement Citywide IT recycling program by **10/31/09.**
- Re-engineer Data Center For Energy Efficiency, Consolidation, & Virtualization by **12/31/09.**
- Consolidate Applications Servers by **12/31/09.**
- Virtualize server farm by **12/31/10.**

Target Outcomes & Measurement

1. 75% reduction in server farm via server consolidation and virtualization.
2. 100% EPEAT (Electronic Product Environmental Assessment Tool) Gold Certification.
3. 100% enforcement of hardware power saving features via System Center Configuration Manager.
4. 20% Total Cost of Ownership (TCO) Reduction in Hardware, Storage, and Backup.
5. 500% Increase in Citywide Processing Power Utilization.
6. 20% Reduction in Data Center Energy Costs.

32. Wireless Field Operations

Project Manager: Barry Jennings, 981-6532

Wireless technology offers significant opportunities to help City staff working in the field. Providing building inspectors, police officers, refuse workers, fire personnel, housing officials, and public health nurses with direct access to back-end systems not only empowers them with the information they need while at a worksite, but also reduces the need for paper reporting and double data-entry.

Mobile computing involves not only selecting appropriate hardware for the field (laptops, tablets, handhelds, etc.), but also the more complicated processes of developing a mobile interface to core business systems and implementing a secure connection to protect information traveling between worksites and the City's internal network. In FY09, the Department of Information Technology will complete the implementation of an upgraded mobile computing infrastructure for the Police Department's entire vehicle fleet and begin mobile computing pilot programs for other City departments, including Fire, Public Works, Housing, Parks, and Planning. By the end of FY10, mobile computing will become an integral part of the City's approach to providing excellent and efficient field services.

Top Business Drivers

1. Increased need for employee mobility in the field.
2. Costly inefficiencies in the way information is transferred to and from the field to the City network (double data-entry, paper reporting, back-and-forth transit time from the field to the office, etc).

FY 2009-2011 Action Items

- Conduct a field wireless pilot, measure performance, and develop an expansion plan by **8/30/08.**
- Adopt a wireless policy that includes security, access, hardware, and software standards by **10/31/08.**
- Specify technical requirements and expand the current City infrastructure to allow for wireless field operations by **10/31/08.**
- Establish standards for physical safeguards to protect against theft or unauthorized access to City Network resources by **11/30/08.**
- Establish methods for tracking and auditing wireless equipment by **12/31/08.**
- Finalize recommendations to expand field wireless technology from cellular connectivity to a wireless local area network (LAN) via Citywide (non-Public Safety) access points by **12/31/10.**

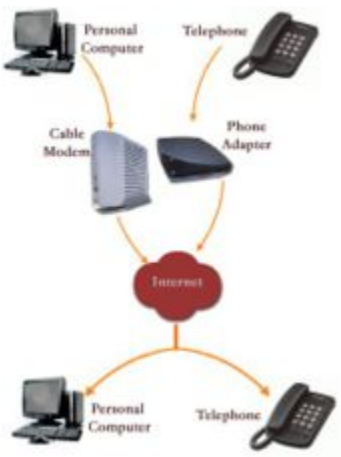
Target Outcomes & Measurement

1. 25% increase in worker productivity as measured by service request completion metrics & self-reporting.
2. 50% reduction in paper reporting and double data entry as measured by service request completion metrics & self-reporting.
3. 25% reduction in transit costs to and from the office, as measure by self-report.
4. 50% reduction in infrastructure costs as measured by savings on cabling costs and labor.

33. Voice / Internet Protocol (VoIP)

Project Manager: Barry Jennings, 981-6532

With the green initiative in the forefront of the minds of City's constituents, Voice over IP (VOIP), or the transmission of voice traffic over data networks, is in prime position for implementation in the '09 fiscal year. Information Technology, in conjunction with the City Manager's office, has been on a mission to strategically consolidate and streamline the City's data infrastructure in an effort to reduce data center energy and administrative costs while simultaneously maximizing the processing output of the City's data systems. With a similar approach to the City's voice network, no longer will voice and data be on two disparate networks requiring separate network infrastructures, but will be unified into an already existing IP data network. Although there will be an initial investment, costs associated with voice will decrease over time and the City of Berkeley will be poised to take full advantage of current and future VOIP technological advances.



Top Business Drivers

1. Costly Telco circuit overhead.
2. Increasing costs associated with two disparate networks.
3. High administrative costs.
4. Increased feature functionality for customers.
5. Preparedness for coming advances in technology.

FY 2009-2011 Action Items

- Produce 2008 IP Telephony Readiness Assessment for the City of Berkeley network by **1/31/09.**
- Design Project Plan with Timelines by **3/31/09.**
- Technology selection & acquisition by **8/30/09.**
- Train IT Administrators in IP Telephony technologies by **9/30/09.**
- Pilot with IT and strategic department partners by **12/31/09.**
- Train all users in new technology by **6/30/10.**
- Rollout to each department in a phased approach by **9/30/10.**

Target Outcomes & Measurement

1. 50% reduction in infrastructure costs over 7 years.
2. Five nines industry standard uptime 99.999%.
3. 30% reduction in administrative costs.
4. 25% reduction in energy costs associated with our voice network.

34. Disaster Recovery

Project Manager: Barry Jennings, 981-6532

A disaster can occur in many forms, from an earthquake to wildfires to a major storm. As the City of Berkeley becomes an increasingly automated organization, the importance of protecting our technical infrastructure and implementing recovery systems to support the City's Emergency Operations Center (EOC) is even more important. Recent improvements to the City's backup and recovery procedures can be expanded to improve our disaster recovery procedures. Replication technologies that allow onver-the-wire transfer of data to secured remote are becoming increasingly less expensive, and provide a powerful option for increasing the robustness of our disaster recovery program. In addition, the emergence of affordable hosted disaster recovery sites and the virtualization of servers give us more flexibility in choosing what we can and cannot do at the remote location.

Top Business Drivers

1. The need to provide business applications and data after a disaster in a reasonable time frame.
2. Current disaster plan not in accordance with first business driver.
3. Commitment to City of Berkeley community and staff for data protection and confidential data.
4. Legislated mandates for increasing robust security and disaster recovery.

FY 2009-2011 Action Items

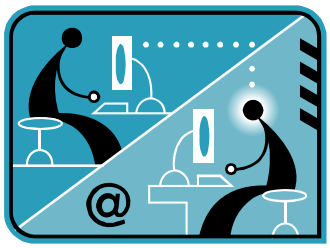
- Train IT staff in basic disaster recovery technologies and methods by **12/31/08.**
- Perform a comprehensive "needs analysis" report for City of Berkeley disaster recovery across all departments by **3/31/09.**
- Perform feasibility study for implementing disaster recovery technologies (including virtualization, fiber, co-location replication, hosted solutions, etc) by **8/31/09.**
- Go to RFP for a comprehensive disaster recovery solution for mission critical applications by **12/31/09.**
- Decide on new disaster recovery solution by **3/31/10.**
- Complete implementation of new disaster recovery solution by **8/31/10.**

Target Outcomes & Measurement

1. 99.999% (Industry Standard 'Five Nines') recovery of critical data and applications in a disaster.
2. 60% reduced reliance on tape for recovery purposes for disaster.
3. 95% increase for time back to business than with tape.
4. 75% decrease in time for administrative tasks than with tape for offsite backup.

35. Standardized Desktops

Project Manager: Sue Sabatino, 981-6553



IT staff are questioned regularly about restrictions imposed on City workstations. We understand the desire to use familiar tools, like the ones at home or at a past job. However, supporting multiple devices and programs that perform similar functions is a costly proposition. This reality is partially analogous to the Police vehicle fleet—learning to repair and stocking parts for Fords, Chevys and Chryslers would be more expensive than maintaining just Fords.

In IT, we have the additional challenges of accounting for the interactions between and the security of whatever technologies are in use. Industry standards in this regard are based on the fact that the most efficient, secure and cost-effective way to deliver computer applications is to serve them to end users from a central source. Ideally, users will interact with applications in a web browser so that no specialized software has to be loaded onto individual workstations. Browser-based services also permit maximum flexibility—they potentially can be configured for access from any Internet connected device, and they can utilize delegated permissions to enable staff and the public to share the same program securely.

Top Business Drivers

1. Imperative to reduce hardware and software acquisition and ownership costs.
2. Urgency to reduce productivity loss arising from compromised workstation software.
3. Pressure to improve security of Computer Network Resources.
4. Reallocation of IT resources to support strategic initiatives.

FY 2008-2010 Action Items

- Implementation of centralized, automated workstation configuration software by **8/31/08.**
- Elimination of end-user Administrator access by **12/31/08**.
- Establishment of hardware standards for mobile computing by **9/30/08**.
- Establishment of an objective process for evaluating requests for exceptions to desktop standards by **12/31/08.**
- Upgrade Microsoft Office 2003 suite by **3/31/09**.
- Pilot implementation of virtualized desktops in at least one City Customer Service Center by **6/30/10.**

Target Outcomes & Measurement

1. Configuration Manager agents verified on 95% of City workstations**.**
2. 15% reduction in annual workstation hardware expenditures**.**
3. 20% reduction in cost of administering PC Replacement Program**.**
4. 90% of City desktops upgraded to most recent City adopted MS Office suite**.**

Glossary

Baseline: Routine technology services that are budgeted in the Department of Information Technology budget and reflect the activities that must get done in order to maintain the City's technical infrastructure (email, telephones, file servers, FUND$).

Business Analysis: The process of systematically and objectively gathering information about business systems and subjecting that information to formal analysis.

Community Relationship Management (CRM): Software that reflects a service model focused on the storage and retrieval of information about customers and community needs in a manner that promotes efficient customer service.

Consolidation: The practice of reducing the number of hardware appliances / software applications throughout an organization and combining them into a centralized system.

Data Warehouse: A central information repository that collects, consolidates, and organizes data to make it more readily available to Citywide business applications, reporting tools, and decision-makers.

Departmental Applications: Major software business applications that one or a few City departments rely upon to guide specific business processes.

E-Government: The use of Internet technology as a platform for exchanging information, providing services, and transacting with citizens, businesses, and other arms of government (also known as e-gov, digital government, or online government).

Enterprise Applications: Major software business applications that all Departments depend upon as the City's core software infrastructure.

Enterprise Licensing: A software site license that typically allows unlimited use of the program throughout the organization.

FUND$: The City's core financial and work management system.

Hardware Sprawl: A situation in which multiple, under-utilized pieces of hardware take up more space and consume more resources than can be justified by their workload.

Integration: The process of physically or functionally linking together different computing systems and software applications.

Interactive Voice Response (IVR): An automated telephony system that interacts with callers, gathers information, and routes calls to the appropriate recipient.

Interoperability: The ability of a system or a product to work with other systems or products without special effort on the part of the customer.

Glossary (Continued)

Middleware: Connects two or more separate software applications, allowing them to "speak the same language" and exchange data.

Non-Baseline: New technology projects meant to improve specific departmental business processes. The start-up costs associated with these sorts of activities must be funded by sponsoring departments / workgroups.

Notice of Interest (NOI): A form that provides the Department of Information Technology with general notice of interest in pursuing a wide-scale technology project so that adequate resources can be scheduled in advance to perform analysis & initiation.

Process Improvement: A methodology for focused change in a business process achieved by analyzing the AS-IS process using process maps and other tools, then developing a streamlined TO-BE process in which automation may be added to result in a process that is better, faster, and cheaper.

Return on Investment: The profits or savings a business will realize from any given use of money.

Scalability: The ability of a computer application or product (hardware or software) to continue to function well when it (or its context) is changed in size or volume in order to meet a business need.

Service Oriented Architecture (SOA): A system's architectural style for creating and using business processes, packaged as services, throughout their lifecycle.

Standardization: The method of establishing uniform technical specifications, criteria, methods, processes, or practices for all hardware and software.

Technology Governance Group (TGG): Formed to ensure a Citywide approach to choosing technology investments and policies. TGG prioritizes "Notice of Interest" submissions from departments interested in pursuing technology projects. TGG comprises two permanent chairs - the Deputy City Manager and the Director of Information Technology - and five rotating chairs open to interested Department Directors.

Technology Infrastructure: Encompasses all information technology assets (hardware, software, data), components, systems, applications, and resources.

Virtualization: Server virtualization is a generalized term describing the ability to host multiple/complete Operating System images (i.e., instances of Windows Server) on a single piece of hardware.

Voice Over Internet Protocol (VoIP): The transmission of voice traffic over wide-area data networks or the Internet (also known as IP Telephony).

Web Content Management: A system that simplifies the publication of Web content to Web sites, allowing content creators to submit content without requiring technical knowledge of HTML. WCM allows for better searches and better-organized content and services so that residents, businesses, and visitors can quickly find what they're looking for.

INFORMATION TECHNOLOGY MASTER PLAN
FY2009—FY2011

Technology Vision: *The City of Berkeley will equip community members and employees with innovative, secure, environmentally sound, and cost-effective technologies to provide excellent municipal services, facilitate civic participation, and help improve the day-to-day lives of community members.*

Elected Officials **Mayor:** Tom Bates **Councilmembers:** Linda Maio (District 1); Daryl Moore (District 2); Max Anderson (District 3); Dona Spring (District 4); Laurie Capitelli (District 5); Betty Olds (District 6); Kriss Worthington (District 7); Gordon Wozniak (District 8); **City Auditor:** Ann-Marie Hogan

City Manager: Phil Kamlarz **Deputy City Managers:** Lisa Caronna & Christine Daniel

RESEARCH & PREPARATION

Donna LaSala, Director, Department of Information Technology

The Technology Governance Group (TGG): **Lisa Caronna,** Deputy City Manager; **Donna LaSala,** Director of Information Technology; **Dan Marks,** Director of Planning & Development; **Claudette Ford,** Director of Public Works; **Fred Medrano,** Director of Health & Human Services; **Tracy Vesely**, Budget Manager

The Technical Policies Team: **Donna LaSala,** Director of Information Technology**; Keith Skinner,** Business Applications Manager**; Nader Kury** Network Operations Manager; **Katrina Holmes,** Information Systems Specialist; **Barry Jennings,** Senior Information Systems Specialist; **Ivan Lapidus**, Senior Information Systems Specialist; **Butch Lavin**, Senior Information Systems Specialist; **Brian McGrath,** Senior Information Systems Specialist; **Sue Sabatino,** Senior Information Systems Specialist; **Mark Gilbert,** Applications Programmer Analyst II; **Ernesto Rodriguez,** Applications Programmer Analyst II

Special Thanks To: **Brian Quinn,** Applications Programmer Analyst II**; Beth Thorman,** Applications Programmer Analyst II; **Eddie Yang**, Applications Programmer Analyst II; **Ken Plante**, Information Systems Support Technician; **Norlinh Stubbs**, Information Systems Support Technician; **Kirk Whitfield**, Information Systems Specialist; **Mary Kay Clunies-Ross**, Senior Management Analyst; **Alicia Abramson**, Library Technology Manager; **Rebekah Lowe**, Senior Systems Analyst

Cover Design: **Amy Lee**, Applications Programmer Analyst I & **Norlinh Stubbs**, Information Systems Support Technician

Editing: **Sue Sabatino,** Senior Information Systems Specialist