BUREAU OF TECHNOLOGY SERVICES ADMINSTRATIVE RULES

Compiled July 3, 2009

Always check individual rules as posted in Portland Online to be sure of the most current iteration.

TABLE OF CONTENTS

BTS-1.01 - Bureau Of Technology Services Vision, Mission, Values, Duties & Authority Of The Chief Technology Officer 2
BTS-1.02 - Administrative Rule Development & 5
BTS-1.03 - Ownership of Information Technology Assets 8
BTS-1.04 - Consolidation Of Information Technology Systems 10
BTS-1.05 - Hardware & Software Maintenance 11
BTS-1.06 - Disposal Of Information Technology Equipment 12

BTS-2.01 - Security Administrative Rule 14
BTS-2.02 - Roles & Responsibilities 17
BTS-2.03 - Network Access 20
BTS-2.04 - Remote Network Access 22
BTS-2.05 - User & Administrative Passwords 24
BTS-2.06 - Database Passwords 27
BTS-2.07 - Virus Prevention & Recovery 29
BTS-2.08 - Incident Reporting & Response 31
BTS-2.09 - Portable Computing Devices 33
BTS-2.10 - Wireless 802.11 Networks 35
BTS-2.11 - Analog Modems 36
BTS-2.12 - Physical Security 38
BTS-2.13 - Intrusion Detection 40
BTS-2.14 - Security Audits 42
BTS-2.15 - Encryption 43
BTS-2.16 - Firewall Security and Management 45
BTS-2.17 - Payment Card Security Standards 46

BTS-3.01 - E-Government Services 50
BTS-3.02 - Web Publishing 53
BTS-3.03 - Web Infrastructure 55

BTS-4.01 - Software Application Life Cycle 56
BTS-4.02 - Shared Data 60
BTS-4.03 - Data Backup 61

BTS-5.01 - Corporate Geographic Information System 63

BTS-6.01 - Technology Definitions 65

BTS-1.01 - Bureau Of Technology Services Vision, Mission, Values, Duties & Authority Of The Chief Technology Officer - Printable Version

BUREAU OF TECHNOLOGY SERVICES VISION, MISSION, VALUES, DUTIES & AUTHORITY OF THE CHIEF TECHNOLOGY OFFICER
Administrative Rule Adopted by Council
ARC-BTS-1.01

BTS Vision Statement
The Bureau of Technology Services (BTS) will enable the delivery of the right information to the right people in the right timeframe using the right resources at the lowest possible cost.

BTS MissionStatement
The Bureau of Technology Services is responsible for providing Information Technology (IT) solutions that best meet the business needs of City government, service to citizens and cost-effective internal operations. The bureau provides efficient, secure infrastructure and software applications that enhance access to information, reduce unnecessary duplication and support City Council's goals and objectives. The Bureau of Technology Services is also responsible for effective management of the City's IT assets and resources and exercises procurement oversight with the Bureau of Purchases.

BTS Values

Strategic Perspective: BTS serves the City best through strategic planning and the anticipation of issues outlined in the ***5-Year IT Strategic Business Plan***, the ***OMF 5-Year Strategic Plan***, and the long-term plans of our customers.

Customer Focus: BTS customers include City bureaus, other Office of Management and Finance corporate bureaus and external business partners. BTS will work with customers and partners to provide the best IT solutions and services to meet defined business requirements, balancing bureau-specific needs and corporate requirements with available resources. Just as the ***5-Year IT Strategic Business Plan*** is designed to minimize disruption, BTS will work in partnership with customers to implement the BTS Administrative Rules.

Coordination & Partnerships: As BTS strives to eliminate duplication of effort and expenditure, increase and ease access to information, and standardize wherever possible, we will actively pursue opportunities for collaboration and cooperation. BTS is committed to regular, effective communication.

Respect & Integrity: BTS values and practices personal and organizational integrity, fiscal and operational accountability, sound management practices, and protection of the public trust.

Knowledgeable, Dedicated Workforce: BTS considers our employees our greatest asset. We strive to maintain a safe and supportive workplace based on principles of accountability and service.

Sustainability: We value, encourage and follow business practices that respect the natural environment and further the City's goals for sustainability.

Responsibility and Authority of the Office of Management and Finance (OMF) - Bureau of Technology Services (BTS) and the Chief Information Officer (CTO)

Ordinance No. 177852 and City Code 3.15 - establishes the Bureau of Technology Services as a bureau of OMF and defines the responsibility and authority of the Chief Technology Officer, effective September 3, 2003.

The Bureau of Technology Services shall be supervised by a Chief Technology Officer (CTO) and shall include such other employees as the Council may provide. BTS shall be responsible for the Information Technology Fund and the Communications Fund.

The Bureau of Technology Services shall:

1. Provide Information Technology strategic planning and consulting services, including budget preparation and analysis, system planning and procurement, resource allocation and project management for information technology projects.

2. Design, implement and manage all IT hardware and software including system security measures.

3. Manage all citywide radio, video, data communications, microwave, wireless communications and telephone systems and equipment owned by the City.

4. Design, implement and manage all citywide voice, video and data applications.

5. Manage end user IT support services, including Help Desk and Desktop Support services.

6. Manage the citywide Geographic Information System.

7. Provide all Internet and Intranet services to City bureaus, offices, boards and commissions.

8. In cooperation with the Bureau of Purchases, review and approve the purchase of all information technology software, hardware and professional consulting services, radio, video, data communication and telephone equipment.

9. Provide citywide communications and electronic consulting for system planning and procurement; written estimates to City bureaus to assist in budgeting; and project management on large systems.

10. Provide all telephone services to City bureaus; coordinate with telephone vendors; order new facilities and equipment for city-owned or leased systems; plan telephone systems, and resolve all telephone problems.

The Bureau of Technology Services will manage and standardize the City's Information Technology and Communications environment in support of the City's business processes.

The Bureau of Technology Services will implement the Technology Services Administrative Rules.

Scope of Administrative Rules

The City of Portland Bureau of Technology Services Administrative Rules is a resource document containing technology related rules.

Some administrative rules shall be promulgated with and administered in conjunction with other bureaus or offices such as the Office of Management and Finance, Bureau of Human Resources and the Portland Office of Emergency Management. Some rules are codified in the Administrative Rules for operational ease, but are administered wholly by other bureaus. The rules will clearly indicate who is responsible for administration.

The provisions of these BTS Administrative Rules apply to all employees of the City of Portland in addition to contractors, vendors, volunteers, and other parties which use and/or support the

City's information and communications systems. In the event of a conflict between the Administrative Rules as they apply to employees and any applicable labor agreements, the latter shall govern.

Violation of Rules
These rules and procedures are to be read in conjunction with federal and state statutes and local ordinances, as applicable.

Violators of BTS Administrative Rules may be denied access to City computing and network resources and may be subject to other penalties and disciplinary action within and outside the City.

Violations will be handled in accordance with the City's established disciplinary procedures. The City may temporarily suspend, block or restrict access to computing resources and accounts, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, confidentiality, or availability of City computing and network resources or to protect the City from liability. The City will refer suspected violations of applicable law to appropriate law enforcement agencies.

In general:
• If violations of this policy initiated by careless or deliberate acts are discovered, the City will take appropriate actions to resolve the issue including disciplinary measures up to and including termination of employment.

• If violations of this policy are discovered that are illegal activities the City, in addition to taking disciplinary measures up to and including termination of employment, the appropriate law enforcement authorities will be notified.
The City reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of any violation of these rules.

Note: Illegal reproduction and/or distribution of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment.

Exception to Rules
Exceptions to the BTS Administrative Rules may be made on a case-by-case basis at the discretion of the CTO in consultation with appropriate BTS managerial staff. In each case, the Bureau must request the exception waiver, in writing, and include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the approval from the Bureau Director requesting the exception.

The CTO has granted exceptions to the Bureau of Water Works & Bureau of Environmental Services SCADA Systems and the Office of Transportation Traffic Management System.

Severability Clause
If any section, subsection, sentence, clause or phrase of the BTS Administrative Rules is found to be invalid by any court of competent jurisdiction, such decisions shall not affect the validity of the remaining portions of these Rules.

BTS-1.02 - Administrative Rule Development & Issuance - Printable Version

ADMINISTRATIVE RULE DEVELOPMENT & ISSUANCE
Administrative Rule Adopted by Council
ARC-BTS-1.02

Purpose
All users of the City of Portland 's information technology systems including employees, contractors, vendors, and other parties, shall have access to rules, procedures and standards related to the proper use, design, testing, implementation, maintenance and replacement of information technologies. The purpose of this rule is to ensure that all official technology rules are accurately formulated, formally approved and documented, in a consistent and accessible manner. Rules must also be distributed in a timely manner to ensure compliance with their objectives and to establish proper accountability.

This document defines what a technology rule is, explains the standardized rule format, outlines the steps for formulating, approving, issuing and amending technology rules, procedures and standards, and establishes the BTS Administrative Rules repository:

http://www.portlandonline.com/auditor/index.cfm?c=26821

Administrative Rule Definition
A citywide Bureau of Technology Services Administrative Rule is binding policy and is defined by all of the following criteria:

• It has broad application throughout the City of Portland
• It helps ensure compliance with applicable laws and regulations, promotes operational efficiency, enhances the BTS mission, and reduces institutional risk
• It mandates or constrains action
• The subject matter requires Council, or Chief Administrative Officer (CAO) review and approval for rule issuance and major change.

Rules shall be approved by the CAO as Council's designee unless otherwise noted in the City Charter. Prior to the adoption, amendment or repeal of any rule, the Chief Technology Officer (CTO) shall give public notice of the proposed action at least fifteen (15) days prior to the effective date by mailing the notice to each council member, all bureau directors and each labor organization representing City employees. The CAO must approve changes in the actual rule once adopted.

Operating Procedures
Any procedural aspect not fundamentally changing the substantive content of an Administrative Rule may be changed at the discretion of the CTO without prior CAO approval.

Standards Definition
Standards are rule-making entities that establish a defined, common, measurable baseline and may be applied to hardware, software, methodology and procedures. Standards are defined to minimize complexity, increase efficiency & security, ease technology procurement and replacement, and communicate a shared technology roadmap. Minimum standards provide binding measurable criteria with which to measure compliance with Rules and Procedures.

Please see section 6.01 Information Technology Definitions for descriptions for the terms used throughout these rules.

Formulating and Approving Citywide Administrative Rules
Development and/or revision of an administrative services rule is the responsibility of the CAO and directors of the citywide administrative services provider bureaus, or their designees, following these steps:

1. A Bureau or Commissioner's Office notifies BTS of the need for a new or revised rule. The CTO may also independently initiate the new rule development process.

2. Develop a problem definition and rule direction statement.

3. Note authority for the rule and any existing rules or policies to be replaced.

4. Identify key stakeholders.

5. Include research of best practices in rule development.

6. Draft rule and provide to CAO for review and initial approval.

7. Distribute draft rule to identified stakeholders for review and comment. The review period will not be shorter than 15 days.

8. Meet with bureaus and other identified stakeholders as needed to receive comments and feedback.

9. CAO formally approves the rule and ensures it is disseminated to Council and to all City bureaus.

Rulemaking Involvement
The Bureau of Technology Services will make every effort to ensure that key stakeholders and external subject matter experts are involved in the framing, formulation and review of new or revised rules. Key stakeholders may include Commissioners and staff, Bureau Directors, technology professionals, labor representatives, employees, and the City Attorney.

Interim Rules
In situations of fiscal or security emergencies, as determined by City Council, the City of Portland CAO may establish procedures or guidelines without seeking such input prior to publication.

Administrative Rule Format
Administrative services rules and policies shall be written in the format designated by the Auditor's Office and indicated by this rule. The rule or policy shall include the following components:

1. The creation date

2. The date of the most recent update

3. Notation of the authority for the rule or policy

4. CAO's initials indicating adoption of the rule or policy

Interpretation of a Rule
The Chief Technology Officer maintains authority for the interpretation and application of Technology Services Administrative Rules.

Bureau Specific IT Management Work Rules
Bureaus may implement bureau specific IT management work rules to assist in day to day operations. Bureau IT work rules may be more restrictive than citywide rules, but cannot be written to provide more latitude. Bureau specific IT management work rules do not require Council approval but are binding on all employees they cover. All drafts of bureau specific IT management work rules must be forward to the CTO for final approval prior to implementation and also to ensure that BTS has a copy of all bureau specific rules in the rule repository.

PortlandPolicy Document Repository
The Auditor shall maintain a copy of all administrative rules and policies in the Portland Policy Documents (PPD) repository. The CAO shall submit an electronic copy of all newly adopted documents to the auditor for inclusion in the PPD within two weeks of implementation.

History
Originally published as PPD number ARC-BIT-1.04, authorized by Ordinance No. 177048 passed by Council and effective November 6, 2002.
Re-indexed by Auditor as PPD number ARC-BTS-1.02.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-1.03 - Ownership of Information Technology Assets

- Printable Version

OWNERSHIP OF INFORMATION TECHNOLOGY ASSETS
Administrative Rule Adopted by Council
ARC-BTS-1.03

Purpose
Consistent, efficient, accountable management and maintenance of the City's Information Technology (IT) environment can best be achieved through consolidated ownership of all corporate Information Technology assets by the Bureau of Technology Services.

A key to the City's ability to work and communicate effectively is dependent on our capacity to gather, analyze and distribute data and information. Maintaining hardware/software assets at a consistent level is essential in order to meet the public's service expectations, conduct efficient business operations, and achieve organizational goals.

The Chief Technology Officer (CTO) is the City's authority for IT issues and related purchases, installation and support matters. As such, the CTO has the responsibility for ensuring interoperability and sustainability of the City's IT components with the City's IT architecture, standards and policies.

Administrative Rule
The Bureau of Technology Services (BTS) owns and manages all IT assets with the exception of assets where it is determined by Council or the CAO to be in the City's best financial interest for a customer bureau to own the asset. IT assets are defined as IT applications, IT systems, and assigned IT equipment.

All new desktop equipment (thick, thin, tiered, client-server, peripheral) for normal business/staff use, must always meet minimum technology standards as defined by BTS.

Responsibility
BTS will charge rates for IT assets. These rates will include a replacement component or a debt service component; unless it is determined by Council or the CAO if it is in the City's best financial interest for a customer bureau to fund replacement resources on its own.

Ownership of IT assets will transition to BTS as assets are replaced. At the time of purchase, the new asset will be booked to the BTS Fund.* This provision shall be fully in effect as of July 1, 2005.

Prior to their time of replacement, IT assets may still be owned by bureaus and their costs booked to the bureau's fund. However, BTS will manage these IT assets during the transition period.

Upgrades of IT assets, or the purchase of additional IT assets, will be funded via cash transfers from the receiver bureau.*

IT equipment will only be purchased by BTS personnel and assigned to bureaus use.* (* or as otherwise determined by Council or the CAO)

History
Originally published as PPD number ARC-BIT-1.06, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.

Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-1.03.

BTS-1.04 - Consolidation Of Information Technology Systems - Printable Version

CONSOLIDATION OF INFORMATION TECHNOLOGY SYSTEMS
Administrative Rule Adopted by Council
ARC-BTS-1.04

Purpose

A consolidated system for IT business processes, including network management, data storage and retrieval, system security, accounting, financial, purchasing, and human resource management systems, enables more efficient monitoring, and management of the City's assets, resources and expenditures. It eliminates continued investment in duplicate systems and processes and lowers costs by reducing the effort required to acquire, transfer, manage and manipulate data

---

Administrative Rule

All existing and future information systems involving use of City owned information that support business processes for accounting, financial, human resources, workflow management, data collection, and data management, will be consolidated into a single, coherent Information Technology (IT) environment, unless specifically exempted by the CTO (or designated representative).

Where services cross Bureau lines, the CTO or designated representative shall decide on how they will be integrated. The CTO or designated representative, working collaboratively with affected bureaus, is authorized to implement the City's standards for system consolidation.

All upgrades to existing corporate administrative services systems - accounting, financial, human resources, purchases, etc - or related application development, shall require review by the CTO (or designated representative), the appropriate corporate business manager* and the CAO.

All other software systems that are or determined to be "corporate systems", over time will require review by the CTO (or designee) and the CAO.

(* Finance Director, Human Resources Director, Purchases Director, etc.)

Responsibility

BTS will work collaboratively with Bureaus to develop and implement retirement/migration plans, for legacy or proprietary systems. System retirement and migration resource requirements will be addressed via the Information Technology Fund.

History
Originally published as PPD number ARC-BIT-1.07, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-1.04.

BTS-1.05 - Hardware & Software Maintenance - Printable Version

HARDWARE & SOFTWARE MAINTENANCE
Administrative Rule Adopted by Council
ARC-BTS-1.05

Purpose
Information technology and data resources are critical assets. The City's ability to effectively deliver services and communicate effectively is dependent on increasing our capacity to gather, analyze and distribute data and information. Maintaining hardware/software assets at the appropriate level is essential to meet the public expectations and achieve organizational goals effectively and efficiently.

The purpose of this policy is to define information technology asset maintenance and replacement expectations.

Administrative Rule
All City owned information technology assets (hardware and software) will be selected and maintained in keeping with BTS established standards while that equipment and software remains in normal business/staff use. Replacement schedules shall be planned for on a cycle that reflects the category and usage of each asset.

Responsibility
Only qualified persons designated or approved by the Bureau of Technology Services may provide hardware and software maintenance support.

The Bureau of Technology Services will provide a level of technical support to City users sufficient to perform their job duties.

In situations where non-City entities and/or personnel use City-owned equipment is involved, the Bureau or Office shall have an agreement outlining such usage and maintenance responsibilities of each party. Additionally, each agreement must be reviewed and approved by the Chief Technology Officer (CTO).

Non-City owned hardware and software will not be maintained by the City unless a prior agreement has been made.

History
Originally published as PPD number ARC-BIT-1.08, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-1.05.

BTS-1.06 - Disposal Of Information Technology Equipment - Printable Version

DISPOSAL OF INFORMATION TECHNOLOGY EQUIPMENT
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-1.06

Purpose

As Information Technology (IT) hardware becomes obsolete or unserviceable, it shall be disposed of or repurposed in a socially responsible and environmentally sound manner, and where applicable, removed from the City's fixed asset inventory.

Additionally, the City has the responsibility to ensure sensitive information is not wrongfully disclosed, nor unlicensed software distributed to unauthorized persons or organizations. Sensitive information includes data that is protected by laws requiring protection of sensitive data from disclosure to individuals or entities outside of the City.

This policy outlines the requirements for properly disposing and/or repurposing of information technology equipment, protecting sensitive information from disclosure and legal obligations regarding software licensing agreements and copyright laws.

Administrative Rule

Disposal of Equipment

IT hardware that has exceeded its planned life cycle, or is no longer cost-effectively serviceable, shall be decommissioned and disposed of in one of four ways at the option of BTS and as it benefits the City:

1) Donation to Portland non-profit organizations

Decommissioned equipment, may be donated to an IRS 501(c)(3) technology hardware recycling organizations, located in the City of Portland, that comply with the City of Portland's Minority/Women/Emerging Small Business, EEO, and other non-discrimination policies. Recipients of equipment donations must commit to recycling donated units to Portland residents, particularly Portland K-12 students, and non-profit organizations that comply with the City of Portland's non-discrimination and EEO policies, free of charge.

All recipient organizations must commit, in writing, to environmentally sound disposal of the equipment through qualified regional recyclers and indemnification of the City from any further responsibility for such equipment.

2) Trade-In

When in the best interest to the City, in course of acquiring required hardware, surplus equipment may be used for trade-in purposes.

3) State surplus

Decommissioned equipment may be sent to the State of Oregon (as a participant to the City's Intergovernmental agreement) for disposal as surplus.

4) Discard

Discarded items may be sent to a facility or organization appropriately qualified for proper disposal or recycling of IT hardware as identified by BTS in collaboration with the Office of Sustainable Development.

Responsibility

Bureau of Technology Services will:

- Determine obsolescence and the decommission schedules of all BTS owned/managed hardware.

- Determine the most appropriate disposal and/or repurposing methods for IT equipment.

- Ensure removal of all City data and software from City hardware in such a manner that it cannot be recovered or reconstructed.

- Ensure secure and environmentally sound disposal of all obsolete BTS owned/managed hardware.

- Document the disposal of all BTS owned/managed Capital Assets.

- Maintain a record of all equipment donations. Records will include indemnification documentation signed by the recipient.

Bureaus will:

- Work with BTS to ensure secure and proper disposal of all bureau owned IT and Telecommunications hardware, rendering all City data unrecoverable and disposing of hardware in an environmentally sound manner.

- Remove all bureau owned/managed systems from the fixed asset inventory.

- Document the disposal of all Capital Assets.

History

Originally published as PPD number ARC-BIT-3.02, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999, passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-1.06.
Revised rule adopted by Chief Technology Officer of Bureau of Technology Services February 2, 2009 and filed for inclusion in PPD June 4, 2009.

BTS-2.01 - Security Administrative Rule - Printable Version

SECURITY ADMINISTRATIVE RULE
Administrative Rule Adopted by Council
ARC-BTS-2.01

Purpose
The purpose of these Information Security Policies is to ensure the security and availability of information technology systems and networks. It also helps ensure confidentiality, integrity and availability of electronic information captured, maintained and used by the City of Portland . This policy shall be used as a foundation document for all policies, standards, procedures, and guidelines that are developed and implemented by the City, related to information security.

The Information Security Policies are to be "living" documents that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives and perceived dangers.

All users (employees, contractors, vendors, and other parties) are expected to understand and abide by these policies.

Authority and Compliance
The Chief Technology Officer (CTO) shall establish and provide authority and governance for information security policies, standards, and best practices for the City technology infrastructure in order to secure all City information systems and assets and promote the most efficient use of technology resources.

The Information Security Manager (ISM) is responsible for developing policies and standards for the implementation and use of information and telecommunications technology security standards and compliance on a Citywide basis.

The City of Portland is a public entity. It has custodial responsibilities for a significant and diverse amount of sensitive information. It holds business contracts with a broad range of public and private organizations. It is the recipient of federal and private grants. It owns, maintains and operates significant critical infrastructures and services including those of public health and safety. All of these facts place significant burden on the City regarding the management and use of its extensive information systems resources. Not least among these burdens are compliance requirements with many State and Federal laws, regulations, and promulgated rules. Pursuant to Federal and State regulations, management control of access to law enforcement data, specifically NCIC 2000 and LEDS, is under the authority of the Chief of Police of the Portland Police Bureau.

Beyond strict compliance requirements, the City must also understand and consider several additional government and industry standards and best practices that contribute to the objective of “due care”.

In addition to the City’s information security governance and compliance requirements, this policy also reflects the City’s strong commitment to its own institutional ethics and values.

Successful compliance and protection of information systems assets requires all business system owners, system operators, data custodians and users of City owned computing, communications and network services, to learn, understand, and support this City’s information security policy and associated guidelines.

Administrative Rule

The Information Security Administrative Rules 2.02 through 2.15 include polices covering the following areas:

2.02: ROLES AND RESPONSIBILITIES
2.03: NETWORK ACCESS
2.04: REMOTE NETWORK ACCESS
2.05: USER & ADMINISTRATIVE PASSWORDS
2.06: DATABASE PASSWORDS
2.07: VIRUS PREVENTION & RECOVERY
2.08: INCIDENT REPORTING & RESPONSE
2.09: PORTABLE COMPUTING DEVICES
2.10: WIRELESS 802.11 NETWORKS
2.11: ANALOG MODEMS
2.12: PHYSICAL SECURITY
2.13: INTRUSION DETECTION
2.14: SECURITY AUDITS
2.15: ENCRYPTION

In addition to the above policies, the following general information security policies apply to all users (employees, contractors, vendors, and other parties) of the City's information systems:

Personnel Accountability: Personnel are accountable for their actions in use of City information technologies and may be held liable to administrative or criminal sanctions for any unauthorized actions found to be intentional, malicious or grossly negligent.

Altering Authorized Access: Personnel are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges and assigned responsibilities.

Unauthorized Access: Personnel are not to access or attempt to access systems or information for which they are not authorized, nor provide access to unauthorized users. Personnel are not to attempt to receive unintended messages or access information by unauthorized means, such as impersonating another system, user or person, misuse of legal user credentials (user ids, passwords, etc.) or by causing any network component to function incorrectly. Personnel are not to possess, intercept or transfer information or communications for which they are not authorized or for which is not an assigned function of their responsibility.

Unauthorized Data Alteration: Entering information into a computer or database that is known to be false and/or unauthorized, or altering a database, document, or computer disk with false and/or unauthorized information is prohibited.

Reconstruction of Information or Software: Personnel are not allowed to reconstruct or duplicate information or software for which they are not authorized.

Malicious Software: Personnel must not willingly or through an act of gross negligence, introduce or use malicious software such as computer viruses, trojan horses, malware or worms.

Tampering with Information Security Software and Settings: Personnel must not tamper with or disable information security software or settings, including but not limited to network password mechanisms, system logs, virus protection software, security auditing and asset management tools, system clocks, screen saver password settings and software distributions tools.

Denial of Service Actions: Personnel are not allowed to prevent authorized users or other systems from performing authorized functions by actions that deny access or the ability to communicate. These include actions that deliberately suppress communications or generate frivolous or unauthorized network traffic.

Software Licenses: All software used on City computers must be appropriately and legally acquired and used according to the licensing agreement. Possession or use of illegal copies of software or data is expressly prohibited.

Protection of Data: Personnel are required to protect the confidentiality, integrity and availability of private or sensitive electronic data they use, transmit and store. Examples of confidential, private or sensitive electronic data include but are not limited to; criminal justice data, pending litigation, employee personnel records health benefits data and medical files, credit card numbers, in-process procurement evaluation and contract negotiation materials, drivers license numbers, social security numbers, dates of birth, intellectual property and all other data expressly exempt from Oregon public records laws provided by ORS 192.501 to 192.505.

Background Checks: Background checks may be a requirement for any employee, volunteer, contractor or vendor who will be working with or around confidential or sensitive IT or communications equipment or data under BTS management. Such determination will be at the discretion of the CTO or delegate in consultation with the ISM, OM and Business System Owner unless it is mandated by law or State/Federal requirement.

Applicability
This Policy is applicable to all Business System Owners, System Operators, Data Custodians, and Users of City computing systems, networks, associated information or any other electronic processing or communications related resources or services.

Exceptions
Exceptions to this policy must be approved by the CTO or delegate in consultation with the ISM and other appropriate BTS management staff. In each case, the bureau must request the exception waiver, in writing, and include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the approval from the bureau director requesting the exception.

Monitoring of User Accounts, Files and Access
Related Administrative Rules governing employee use of information technologies and expectation of privacy, monitoring of use, site blocking, prohibited use, E-mail (including all-employee broadcast E-mail, Union use of E-mail, Netiquette, and Email records retention), and virus protection are included in the Bureau of Human Resources Administrative Rules.

Electronic Data and Records Management
Vast amounts of electronic data are in use and stored in many different forms, on computing systems and diverse data storage media. Elements of this data comprise records that are official City records. ***Records Retention and Disposition Schedules*** are promulgated by the City Auditor's Office and can be located at http://www.portlandonline.com/auditor/

All City Business System Owners, Data Custodians, and Users are obligated to understand the nature of the data they generate, use, or store and ensure that they are managing that data in full compliance with City records management policies.

History
Authorized Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.02 - Roles & Responsibilities - Printable Version

ROLES & RESPONSIBILITIES
Administrative Rule Adopted by Council
ARC-BTS-2.02

Purpose
Responsibility for protecting City information systems and data is shared by many entities and individuals throughout the City including Business System Owners, System Operators, Data Custodians, Users and the Information Security Manager.

The purpose of this policy is to describe the specific roles and responsibilities of each of these groups and individuals with regards to Information Security.

Role & Responsibilities

Information Security Manager
The Information Security Manager provides a key role of centralized oversight, direction, and support for all information systems security-related services for the City. These responsibilities include, but are not limited to the following key areas:
• Support for City security policy development, implementation, and enforcement.
• Support for strategic security planning and plan implementation.
• Support for security awareness and education programs.
• Incident response services as needed.
• Security consulting services as needed.
• Support for the development and implementation of all appropriate security standards and guidelines as necessary for the City.

Users
All Users have a critical role in the effort to protect and maintain City information systems and data. Users of City computing resources and data have the following responsibilities:
• Support compliance with all federal and state statutes and regulations.
• Comply with all City and Bureau policies and guidelines.
• Protect all City assets and never share access accounts, privileges and associated passwords.
• Maintain the confidentiality of sensitive information to which they are given access privileges.
• Accept accountability for all activities associated with the use of their user accounts and related access privileges.
• Ensure that use of City computers, email, internet access, computer accounts, networks, and information stored, or used on any of these systems is restricted to authorized purposes and defined acceptable use policies.
• Report all suspected security and/or policy violations to an appropriate authority (e.g. manager, supervisor, BTS Helpdesk, Information Security Manager).
• Follow all specific policies, guidelines and procedures established by individual City bureaus and offices as well as agencies with which they are associated and that have provided them access privileges.

Business System Owners
Business System Owners play a critical role in the protection of City information systems and data. Business System Owners have responsibility for their owned systems and shall:
• Ensure compliance with all City and Bureau policies, standards and guidelines as well as all statutory and regulatory requirements.
• Define the criticality of assets and the level of security required for protection. This is determined by performing a business impact analysis of the critical functions as determined within the asset criticality guidelines
• Assign and provide necessary support and authority to appropriate staff to carry out the functions of Data Custodian(s) for all systems owned. Work in cooperation with other Business

System Owners for shared systems to ensure that Data Custodian responsibilities are properly fulfilled.
• Ensure the confidentiality of sensitive proprietary data especially personally identifiable information, protected criminal justice information, and sensitive information related to protection of critical infrastructure.
• Ensure that access granted to users is based on the “Principle of Least Privilege” and “Principle of Separation of Duties” where required.
• Ensure that all incidents of security breaches are documented and reported to BTS and security services personnel.
• Document and submit any desired exceptions to citywide policy for review to the CTO.
• Support all incident response activities that involve their system(s).
• Advocate for security resources as required in City budget processes and in grant proposals.
• Define the business parameters for disaster recovery plans, including both the required recovery time and the required recovery point.
• Ensure all new employees and those granted access to City information systems read, understand and abide by all City policies, standards and guidelines
• Provide timely notification to BTS, System Operators and Data Custodians in events where access to City information systems is no longer required. Such events include employment termination or job duty change.

Data Custodians

The role of Data Custodians is to provide direct authority and control over the management and use of specific information or data. The Data Custodian may be a Supervisor, Manager, or designated professional staff, assigned the responsibility by the Business Owner (Bureau Director). They may serve dual roles as a System Owner/Operator as well as a Data Custodian; however, this practice should be limited consistent with the principle of separation of duties, such that they typically would not be the technicians (system administrators) that support the related computer systems or applications. Their responsibilities include:
• Ensure compliance with all citywide and Bureau policies and all statutory and regulatory requirements.
• Provide the requirements for all access control measures related to the data they are charged with protecting to the System Operators.
• Support access control to data by acting as a single control point for all access authorization. Maintain data access authorization documentation. This document should be reviewed with the System Operator.
• Support regular review and control procedures to ensure that all users and associated access privileges are current, accurate and appropriate.
• Ensure that access granted to users is based on the “Principle of Least Privilege” and “Principle of Separation of Duties” where required.
• Ensure that data backup and retention requirements are aligned with business needs and public records rules maintained by the Auditors Office (http://www.portlandonline.com/auditor/).
• Notifies the appropriate system operators when access granted to users is no longer required.
Data Custodians must work in conjunction with System Operators and the Information Security staff to ensure that “due care” is taken to properly protect sensitive data.

System Operators

The role of System Operators is to provide day-to-day operation of a server or system. System operators, or sometimes referred to as system administrators, have the following responsibilities:
• Works with the customer (business system owner and data custodian) to understand specific security requirements as they relate to business criticality
• Works with customer (Business System Owner and Data Custodian) to identify appropriate user access to the system and data
• Works with Information Security personnel to effectively implement technologies and configurations which comply with information security policies, standards, guidelines and procedures.
• Establishes, prior to implementation, appropriate account access, technical support access, as well as backup and emergency support.

• Ensures, as appropriate, that physical and logical access security is always controlled and that robust backup and recovery mechanisms are employed.
• Regularly monitors for unauthorized access as well as maintains a history file for auditing purposes and reports any unauthorized or suspicious activity immediately to information security personnel.
• Works with the Business System Owner and Data Custodian in preparing disaster recovery plans.
• Works with the Data Custodian to define the proper data backup and retention schedule and ensures data is consistently backed up and retained in accordance with such schedules.
• Removes access to City information systems immediately upon notification of proper events such as employee termination or reassignment of job duties.

History
Authorized Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.03 - Network Access - Printable Version

NETWORK ACCESS
Administrative Rule Adopted by Council
ARC-BTS-2.03

Purpose
Access to resources on the City network is essential for many City employees to do their job. At the same time, security considerations require that access is limited to only those persons whose responsibilities require access, and to only those resources required to fulfill their duties.

The purpose of the Network Access Policy is to establish rules for the access and use of the City's network infrastructure.

Administrative Rule
Access to the City's network and applications will be made available to all Bureaus, Offices and locations and follow a standard process to determine access requirements for:
• City personnel
• Citizens and business partners
• Contracted support personnel

City employees will be given access to only those specific resources actually required to accomplish their job as determined by Business Systems Owners and Data Custodians.

Non-City employees will not be given access to the City's network, except on a case-by-case basis or by Council action (e.g. Intergovernmental Agreements). Any non-City employee receiving permission to access the City's network must abide by all City Information Technology policies, standards and procedures.

Security-warning banners must be displayed prior to allowing the logon process to be initiated by users. This security banner must inform all users that the network being accessed is proprietary, should only be accessed by authorized users, and that system use is monitored for enforcement purposes.

Responsibility

Bureau Responsibilities
• Business System Owners and Data Custodians shall identify those employees who require access to the City network, including specific network resources and applications. These approved authorizations shall be in writing and maintained by BTS.
• Business System Owners and Data Custodians shall identify the minimum required account access required for an employee to effectively fulfill their responsibilities.
• For non-City employees, the responsible Bureau Manager must identify network access requirements with proper written justification and receive prior approval from the CTO or delegate in consultation with the Information Security Manager and Operations Manager. Requests for such access can be made by completing the appropriate request form. http://www.portlandonline.com/omf/index.cfm?c=39147
• Business System Owners and Data Custodians or a designated Bureau of Human Resources representative, are responsible for immediately notifying the BTS Helpdesk when access to City information systems should be discontinued. Specific examples included termination of employment or assignment to responsibilities and duties for which access is no longer required.
• Data Custodians, or those who manage Bureau specific data which can be accessed by multiple users, are responsible to conduct bi-annual audits to ensure assigned users continue

to require access. Any required changes of access rights should be immediately reported to the Bureau of Technology Services.

Bureau of Technology Services Responsibilities

• Create and delete user accounts, grant and revoke access to appropriate computing resources as defined by the Business System Owners and Data Custodians following established policies and procedures.
• Disable all user accounts found to be inactive for a period of 90 days.
• Delete all user accounts that have been disabled for a period greater than 1 year.
• Respond to bureaus for specific help needed to audit network access.

History

Originally published as PPD number ARC-BIT-2.04, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-2.03.

BTS-2.04 - Remote Network Access - Printable Version

REMOTE NETWORK ACCESS
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.04

Purpose

Remote network access is a generic term used to describe accessing an organization's computer network by individuals not located at the organization's offices. This may take the form of traveling employees, employees who regularly work from home, or employees who work both from the office and from home. In many cases, both the organization and the employee may benefit from the increased flexibility provided by remote access. As with any innovation, however, the benefits may be countered by risks if the purposes and methods of the remote access are not fully understood by all participants.

The purpose of this policy is to define the approved method for City employees and approved vendors and contractors, to remotely connect to the City network and how their connection will be established, controlled and managed.

Administrative Rule

City employees, vendors and contractors have the capability to remotely access the City's network. This access may be suspended or terminated based on Bureau or Office management request or BTS determination that remote network access has been misused or has compromised the City's information security. The approved method of remote access is through a Virtual Private Network (VPN) connection.

The following policies apply to utilizing remote VPN access to the City's network:

- When actively connected to the City network, the City's VPN will force all traffic to and from the remote computer over the VPN tunnel. All other traffic will be dropped. Split tunneling is not permitted; only one network connection is allowed.

- Remote VPN users assume the responsibility to assure that unauthorized users do not access City networks through their systems, software or configurations. This includes employee's family members, friends and associates.

- Security measures, such as a patched operating system, a current personal firewall, and current anti-virus software are required to prevent unauthorized access to the City's network. Additional security measures, such as strong authentication technologies, are also required for those users who seek to remotely access internal City network resources.

- For non-City employees such as vendors and contractors, the responsible Bureau Manager must identify and approve remote network access requirements with proper written justification.

Exceptions to this policy, or any sections thereof, may be granted on a case-by-case basis by the CTO or the Information Security Manager. Users who access the City's network via non-City computers understand that their computers are a de facto extension of the City's network and as such, are subject to all the same policies that apply to City employees and City owned and managed computing equipment.

Responsibility

The Bureau of Technology Services is responsible for setting up remote VPN access in a manner that is consistent with information security standards and policies. Such standards and policies include current virus protection software, operating systems, operating systems patches, firewalls as well as other security and remote administration tools, such as strong authentication technologies. The Information Security Office is responsible for maintaining these technologies; as well as providing policy, procedure, and configuration guidance related to remote network access.

History

Originally published as PPD number ARC-BIT-2.05, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999, passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-2.04.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 5, 2009.

BTS-2.05 - User & Administrative Passwords - Printable Version

USER & ADMINISTRATIVE PASSWORDS
Administrative Rule Adopted by Council
ARC-BTS-2.05

Purpose
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may easily result in the compromise of the City's entire network. As such, all City employees (including contractors and vendors with access to City systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, the association of passwords with user accounts and the frequency of password changes.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City facility, has access to the City network, or stores any non-public City information.

Administrative Rule
• Each approved City user is to be issued a unique user account and password. In general, sharing of user accounts and passwords is prohibited. BTS will work with bureaus who request an exception to this rule or to assist them in implementing more secure methods to address requirements met by sharing user passwords.

• All shared administrative or system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.) must be changed at least once every 90 days or immediately when an employee with knowledge of the password terminates employment with the City or is reassigned to responsibilities in which such knowledge is no longer required.

• All user-level passwords (e.g., network login, email, web, IBIS, desktop computer, etc.) must be changed at least every 180 days. Note: User accounts with access to data protected under legal regulations such as Criminal Justice Information Systems (CJIS) Policy, etc., may be subject to more restrictive password requirements.

• User accounts that have system or administrative level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user. Additionally, all such passwords must be changed at least once every 90 days.

• System level/administrative access and general user access must be conducted via separate and unique user accounts. Systems operators must not use system or administrative level accounts for general office use (reading email, browsing the internet, etc). General office access must be accomplished via non-system level accounts. This does not apply to users specifically granted administrative level access to their personal workstation.

• Passwords must not be inserted into email messages or other forms of electronic communication. Leaving a password as a message on a users confirmed voicemail is acceptable however care must be taken to make sure such passwords are not overheard by anyone other than the intended recipient.

• Where supported by the system, all passwords must be at least 8 characters in length and contain at least 3 of the following 4 characteristics:
o Lowercase letters (ex. a, b, c)

o Uppercase letters (ex. A, B, C)
o Numbers (ex. 1, 2, 3)
o Special characters (ex. !, @, #)
• Where supported by the system, all accounts must be automatically locked out after no more than 10 incorrect password attempts within a 30 minute time window and must remain locked for a minimum of 30 minutes unless unlocked by authorized BTS support personnel.

• Where supported by the system, all new passwords must not be a repeat of a previously used password within the last 10 password change events.

• Where supported by the system, all workstations and file servers must implement an automatic password protected screen saver after no more than 15 minutes of keyboard or mouse inactivity.

• Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

• When a user account is created with a default password, or is reset by authorized BTS personnel, the password must be set to expire and be changed at the next logon.

• If someone demands you reveal your password, do not do so. Refer them to this document or have them call the BTS Helpdesk in order to appropriately request access to City information systems and/or data.

• If an account or password is suspected to have been compromised, report the incident to BTS Helpdesk and change all passwords immediately.

Guidelines

Password Construction
Passwords are used for various purposes at the City. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection and network equipment logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:
• The password contains less than eight characters
• The password is a word found in a dictionary (English or foreign)
• The password is a common usage word such as:
o Names of family, pets, friends, co-workers, fantasy characters, etc.
o Computer terms and names, commands, sites, companies, hardware, software.
o The words "portland ", "seattle ", "sanfran" or any derivation.
o Birthdays and other personal information such as addresses and phone numbers.
o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
o Any of the above spelled backwards.
o Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
Strong passwords have the following characteristics:
• Contain both upper and lower case characters (e.g., a-z, A-Z)
• Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
• Are at least eight alphanumeric characters long.
• Are not a word in any language, slang, dialect, jargon, etc.
• Are not based on personal information, names of family, etc.
• Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title,

affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
NOTE: Do not use either of these examples as passwords BTS will work with Bureaus in the implementation of strong passwords.

Password Protection
Do not use the same password for City systems as for other non-City systems (e.g., personal ISP account, option trading, external email, etc.). Where possible, don't use the same password for various City access needs. For example, select one password for the mainframe system and a separate password for the network system. Also, select a separate password to be used for a Windows account and a Unix account.

Here is a list of "don'ts":
• Don't reveal a password over the phone to anyone
• Don't reveal a password in an email message
• Don't reveal a password to your boss
• Don't talk about a password in front of others
• Don't hint at the format of a password (e.g., "my family name")
• Don't reveal a password on questionnaires or security forms
• Don't share a password with family members or friends
• Don't reveal a password to co-workers while out sick, traveling or on vacation
In general, it is not advised to use the "Remember Password" feature of applications (e.g., Internet Explorer, etc) as these leave your password vulnerable on the systems they are stored. This is of particular concern on shared systems such as kiosks. Where a City application has a specific ability to retain a password, this function may be used understanding the above mentioned risks.

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system (including Palm Pilots or similar devices) without BTS approved encryption technologies.

Compliance
Password cracking or guessing, using commonly available methods, may be performed by the Information Security Office in cooperation with BTS Operations, on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it immediately.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.06 - Database Passwords - Printable Version

DATABASE PASSWORDS
Administrative Rule Adopted by Council
ARC-BTS-2.06

Purpose
This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program or application that will access a database running on one of the City's networks.

Computer programs running on the City's networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

This policy applies to all programs and applications that will access a City, multiuser production database using a stored credential. An example of this scenario is a web server or batch processing system authenticating to a database server for the purpose of processing database queries on behalf of a user. This policy does not apply to interactive end-user or administrative passwords used to access City applications or databases which are covered by Rule 2.05 END USER & ADMINISTRATIVE PASSWORDS.

Administrative Rule

General
In order to maintain the security of the City's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text.

Specific Requirements
Storage of Database 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/everyone 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 must not be stored in a location that can be accessed externally through a web browser.
• Passwords or pass phrases used to access a database must adhere to BTS Rule 2.05: USER & ADMINSTRATIVE PASSWORDS.
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 you may store database credentials must be physically separated from the other areas of code, e.g., 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 browseable or executable file directory tree in which the executing body of code resides.

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.
• Database passwords used by programs are system-level passwords as defined by BTS Rule 2.05: USER & ADMINSTRATIVE PASSWORDS.
• Database user names and passwords used by programs, such as a web server connecting to a database, must not also be used for interactive sessions by end users or system operators.
• Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with BTS Rule 2.05: USER & ADMINSTRATIVE PASSWORDS. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

History

Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.07 - Virus Prevention & Recovery - Printable Version

VIRUS PREVENTION & RECOVERY
Administrative Rule Adopted by Council
ARC-BTS-2.07

Purpose
Computer viruses can be transferred by disk, local and wide area networks, connections to the internet, email and by a variety of other means. Computer viruses can quickly spread to destroy or corrupt data. Overall service to internal and external customers of Bureaus and Offices can be drastically affected by contracting a computer virus. Diligence demands stringent efforts to safeguard City owned and managed systems and data from viruses.

This policy applies to all computers, systems and network devices connected to City networks to ensure effective virus prevention, detection and eradication.

Administrative Rule
All systems connected to City owned networks must have BTS approved virus protection software, operating systems, operating system patches, applications and application patches installed, operational and up-to-date at all times.

Responsibilities
Bureau of Technology Services Responsibilities
• Procurement, installation, maintenance and monitoring of virus prevention software, operating systems, operating system patches and equipment in accordance with City standards and to institute measures to ensure that virus prevention methods remain current.
• Maintain procedures for proactively preparing for and reactively responding to, virus outbreaks to minimize City impact and restore full operations as quickly and securely as possible.
• Isolate or quarantine systems and/or network segments to prevent and /or contain virus outbreaks, minimize impact and to effectively restore services in a timely manner.
• Implement technologies as funding is available and establish policies and procedures that limit the methods of connections for networked devices (laptops, PDA's, etc) that do not meet minimum security standards and specifications.
Bureau & User Responsibilities
• Comply fully with all virus security actions, warning and notices as issued by the Bureau of Technology Services.
• Do not open email file attachments from an unknown or untrustworthy source or from known sources when the messages appear suspicious in nature.
• Report all suspected virus incidents or missing/malfunctioning virus protection software immediately to the Bureau of Technology Services Helpdesk.
• Logoff all personal computing systems from the City network at the end of each normally scheduled work day so as to ensure current virus signature updates.
• As noted in BHR Administrative Rule Section 4.08, do not download and/or install software on City computers without prior approval from BTS.
• Do not connect any non-BTS supported computer or network device to the City network without prior validation and authorization from BTS.
• Do not circumvent, disable or remove any BTS virus protection software, systems or patches.
• Fund replacement of bureau owned aging equipment (servers/workstations) when it no longer supports BTS standard operating systems versions, virus protection software or patches (virus or application) required to maintain adequate virus security on such equipment.

Supporting Practices

With assistance from the Bureau of Technology Services, Bureau and Office managers shall ensure that employees are provided with information on safe practices for virus protection and that these safe practices are observed at all times.

As per BHR Administrative Rules Section 4.08, City employees are reminded of the expectation to observe safe practices regarding the use of computers to minimize the risks of viruses.

History
Originally published as PPD number ARC-BIT-2.03, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-2.07.

BTS-2.08 - Incident Reporting & Response - Printable Version

INCIDENT REPORTING & RESPONSE
Administrative Rule Adopted by Council
ARC-BTS-2.08

Purpose
Compromises in security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems in the City. Incidents can be accidental incursions or deliberate attempts to break into systems and can be benign to malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of individuals and the City as a whole.

For the purposes of this policy an "Information Security Incident" is any accidental or malicious act with the potential to result in misappropriation or misuse of confidential information (social security number, health records, financial transactions, etc.) of an individual or individuals, significantly imperil the functionality of the information technology infrastructure of the City, provide for unauthorized access to City resources or information, allow City information technology resources to be used to launch attacks against the resources and information of other individuals or organizations.

In the case an information security incident is determined to be of potentially serious consequence, the responsibility for acting to resolve the incident and to respond to any negative impact rests with the BTS Information Security Office in cooperation with the Chief Technology Officer and BTS Operations Manager rather than other specific individuals, bureaus, departments, or groups. The City has established procedures and identified the Information Security Manager (ISM) as its authority in developing response plans to serious information security incidents. As described below, reports of information security incidents will be forwarded to the ISM. The ISM follows protocols in determining what actions should be taken and depending upon the nature of the security incident will determine whether incidents should be handled within the purview of the bureau, HR, or by additional security and operations specialists within BTS or the Information Security Office. In some cases, the ISM may escalate the incident to the City Attorney, law enforcement, human resources or other City officers.

This policy outlines the procedures individuals should follow to report potentially serious information security incidents. City employees whose responsibilities include managing computing and communications systems have even greater responsibilities. This document outlines their responsibilities in securing systems, monitoring and reporting information security incidents, and assisting individuals, administrators, and other BTS staff to resolve security problems.

Administrative Rule
All City employees shall take appropriate actions to report and minimize the impact of information security incidents.

Reporting unlawful or improper actions of City employees is expected and covered in the following Bureau of Human Resources Administrative Rules:

BHR-11.01: STATEMENT OF ETHICAL CONDUCT
BHR-11.02: PROHIBITED CONDUCT
BHR-11.03: DUTY TO REPORT UNLAWFULL OR IMPROPER ACTIONS

To review the rules, access the Auditor's web site at:
http://www.portlandonline.com/auditor/index.cfm?c=26812

Responsibilities

City Employees

• Should attempt to stop any information security incident as it occurs. Powering-down the computer or disconnecting it from the City network may stop or contain any potentially threatening activity.
• Report information security incidents immediately to the BTS Helpdesk. BTS support staff will help you assess the problem and determine how to proceed.
• Following the report, individuals should comply with directions provided by BTS support staff and/or the ISM to repair the system, restore service, and preserve evidence of the incident.
• Individuals should not take any retaliatory action against a system or person believed to have been involved in an information security incident.

BTS Support Professionals

BTS technology professionals have additional responsibilities for information security incident handling and reporting for the systems they manage. In the case of an information security incident, BTS support staff should:
• Respond quickly to reports from individuals.
• Take immediate action to stop the incident from continuing or recurring.
• Determine whether the incident should be handled locally or reported to the ISM.
• If the incident does not involve the loss of confidential information or have other serious impacts to individuals or the City, the support specialist should:
1. Repair the system, restore service, and preserve evidence of the incident.
2. File an Information Security Incident Report Form including a description of the incident and documenting how it was resolved. http://www.portlandonline.com/omf/index.cfm?c=39147
• If the incident involves the loss of confidential information or critical data or has other potentially serious impacts, the support specialist should:
1. Contact the Information Security Office immediately. The ISM or a delegate will investigate the incident in consultation with the CTO, BTS Operations Manager and relevant technology support specialists and develop a response plan.
2. File an Information Security Incident Report Form including a description of the incident and documenting any actions taken thus far.
http://www.portlandonline.com/omf/index.cfm?c=39147
3. Notify the BTS Operations Manager or delegate that an incident has occurred and that the Information Security Office has been notified.
4. Refrain from discussing the incident with others until a response plan has been formulated.
5. Follow the response plan from the ISM to:
• Repair the system(s) and restore service.
• Preserve evidence of the incident.
• Support staff should not take any retaliatory action against a system or person believed to have been involved in an information security incident.

History

Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.09 - Portable Computing Devices - Printable Version

PORTABLE COMPUTING DEVICES
Administrative Rule Adopted by Council
ARC-BTS-2.09

Purpose
Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop and laptop devices in a wide number of applications. However, the portability and small size offered by these devices may increase the security exposure to organizations using such devices.

The purpose of the City's Portable Computing Security Policy is to establish the rules for the use of portable computing devices and their connection to the City network. These rules are necessary to preserve the integrity, availability and confidentiality of City information and assets.

This policy covers all portable computing devices (PDA's, Blackberries, Smart Phones, etc) owned, maintained and operated by the City.

Note: Laptop and notebook computers do not apply to this policy, however they are covered under all the same policies applicable to desktop computers & workstations.

Administrative Rule

• Only BTS approved portable computing devices may be used to access City information systems.

• All portable computing devices must be registered with the BTS Operations group's asset management system and included asset tags or other identification markings for tracking which are required per City accounting policy. Please note, personal identification markings which could inform a thief of the nature of sensitive material stored on any personal computing device, should be avoided.

• Where technically feasible, all portable computing devices must be password protected and have an inactivity timeout. Any devices with non-public information shall have enabled a lock-out feature to restrict the number of password guesses and comply with all other City password policies or shall use encrypted storage for non-public information.

• All portable computing devices which access the City network (other than synchronization with a City desktop or laptop) must have BTS approved antivirus products and firewalls operational at all times to prevent propagation of malicious code (viruses, trojans, worms, etc.).

• In general, sensitive City data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive City data must be encrypted using BTS approved encryption techniques.

• SensitiveCity data must not be transmitted via wireless to/or from a portable computing device unless BTS approved wireless transmission protocols along with approved encryption techniques are implemented.

• All remote access to the City network must be either through a City approved access gateway or via an Internet Service Provider (ISP).

• Non-City portable computing devices that require network connectivity must conform to City information security policies and standards and must be approved in writing by the CTO or delegate in consultation with the Information Security Manager and Operations Manager.

• AllCity employees must be responsible to secure portable computing devices in their care and possession and immediately report any loss or theft of such devices to their bureau management. Additionally, if such devices support connectivity to the City network, the BTS Helpdesk should be contacted to take immediate steps to protect against unauthorized access to the City's information assets.

Guidelines

• When not in use, external wireless communication mechanisms such as 802.11 or Bluetooth, should be turned off.

• Beware of shoulder surfers. When people peer over your shoulder in the airport or other public places, they may be trying to see confidential data or watch you type in a password. When possible, use a polarizing screen cover which helps prevent viewing the display screen from side angles.

• When conducting City business wirelessly, without VPN technologies, Wi-Fi access points (such as those at coffee shops) should be avoided since they may not have all the proper security features enabled.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.10 - Wireless 802.11 Networks - Printable Version

WIRELESS 802.11 NETWORKS
Administrative Rule Adopted by Council
ARC-BTS-2.10

Purpose
This policy prohibits access to City networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or those which have been granted an exclusive waiver by the CTO or delegate in consultation with the Information Security Manager (ISM), ComNet Manager and Operation Manager (OM) are approved for connectivity to the City's networks.

This policy covers all 802.11 wireless data communication devices (e.g., personal computers, laptops, notebooks, PDA's, etc.) which connect to any of the City's internal networks or systems.

Administrative Rule

Register Wireless Devices: All wireless devices (Access Points, Base Stations and Network Interface Cards) connected to the City network must be approved, registered, installed and maintained by the Bureau of Technology Services (BTS).

Encryption and Authentication: To connect to the City network, all computers with wireless LAN devices must utilize a City approved configuration which drops all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point-to-point hardware encryption of at least 128- bits. All implementations must support a hardware address (MAC address) that can be registered and tracked. All wireless implementations must support and employ strong user authentication which checks against a BTS approved and managed RADIUS database and support 802.1x authentication.

Setting the SSID: All wireless access points shall have their SSID configured so that it either is not broadcast or does not contain any identifying information about the City, such as the bureau name, department title, employee name, building location or product identifier.

Penetration Tests and Audits: Wireless Access Points & Base Stations are subject to periodic penetration tests and audits. Unapproved wireless access points and/or those devices which do not comply with BTS approved security configurations are subject to immediate network disconnection and equipment confiscation.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006

BTS-2.11 - Analog Modems - Printable Version

ANALOG MODEMS
Administrative Rule Adopted by Council
ARC-BTS-2.11

Purpose
This document explains the City's analog modem acceptable use and approval rules and procedures. This policy covers the use of modems that are to be connected to computers and computing devices.

This rule covers only those modems that are to be connected to a device inside City buildings and testing sites. It does not pertain to modems that are connected into employee homes, PBX desktop phones, wireless modems used in portable computing devices or fax machines.

There are two important scenarios that involve modem misuse, which we attempt to guard against through this policy. The first is an outside attacker who calls a set of phone numbers in the hope of connecting to a computer or system which has a modem attached to it. If the modem answers (and most computers today are configured out-of-the-box to auto-answer) from inside City premises, then there is the possibility of breaching the City's internal network through that computer, unmonitored. At the very least, information that is held on that computer alone can be compromised. This potentially results in the loss of sensitive City information.

The second scenario is the threat of anyone with physical access into a City facility being able to use a modem equipped computer. In this case, the intruder would be able to connect to the trusted networking of the City through the computer's ethernet connection, and then call out to an unmonitored site using the modem, with the ability to siphon City information to an unknown location. This could also potentially result in the substantial loss of vital information.

Administrative Rule
The general policy is that requests for computers or other intelligent devices to be connected to modems from within City will not be approved for security reasons. Modems represent a significant security threat to the City, and active penetrations have been launched against such lines by hackers. Waivers to this policy may be granted on a case by case basis.

Procedure

Requesting an Modem Connection
Once approved by a Bureau Director, the individual requesting a modem connection must provide the following information:
• A clearly detailed business case of why other secure connections available at the City cannot be used
• The business purpose for which the modem is to be used
• The software and hardware to be connected to analog phone line and used across the line
• To what external connections the requester is seeking access.
The business case must answer, at a minimum, the following questions:
• What business needs to be conducted over the modem?
• Why a City equipped desktop computer with Internet capability is unable to accomplish the same tasks as the proposed modem?
In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:
• Will the machines that are using the modem be physically disconnected from City's internal network?
• Where will the modem be placed? An office, cubicle or lab?

• Is dial-in from outside of the City required?
• How many modems are being requested, and how many people will use them?
• How often will the modem be used? Once a week, 2 hours per day, etc?
• What is the earliest date the modem can be terminated from service as the modem must be removed as soon as it is no longer in use.
• What means will be used to secure the modem from unauthorized use?
• What types of protocols will be run over the modem and analog line?
• Will BTS approved anti-virus software be installed on the machine(s) using the modem?
The requester should use the Analog Modem Request Form to address these issues and submit the request to the BTS Helpdesk. http://www.portlandonline.com/omf/index.cfm?c=39147

The Chief Technology Officer (CTO) or delegate, in consultation with the Information Security Manager (ISM), ComNet Manager and Operations Manager (OM) will review and rule on all analog modem requests

---

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.12 - Physical Security - Printable Version

PHYSICAL SECURITY
Administrative Rule Adopted by Council
ARC-BTS-2.12

Purpose
This policy describes the methods and responsibilities for protecting physical computer, network, communications and information resources. The City requires that appropriate environmental, protection and access controls be in place to protect computing and information resources. Proper and adequate physical security and protection is the responsibility of all City employees.

Physical Security
Physical security measures are an important part of any effort to protect information system assets and services. As with logical security measures at the City, physical security measures required for protecting City computing resources shall be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved. Control measures will be applied in accordance with systems environment sensitivity and criticality.

The City has a wide spectrum of information systems deployments. They include:
• Desktop computer workstations and printers operated in an office environment.
• Wireless and mobile devices such as laptops, radios, mobile data computers, cellular phones and personal digital assistants (PDA's) which are operated both in an office environment and at remote locations.
• Small sets of individual Bureau servers located in office environments.
• Computer labs which host computing and network equipment used for testing and development purposes.
• Telecommunications closets which contain network and communications equipment and wiring.
• Media storage areas or vaults which are used to store electronic media such as backup tapes, surplus equipment and classified documents.
• Modest-sized server rooms which host a limited number of computing devices and networking equipment.
• Enterprise data center facilities that host a wide variety and large quantity of critical computing equipment such as mainframes, servers, tape libraries, storage arrays and network equipment.
All of these technology deployments require varying levels of physical security commensurate with the criticality of the systems and information involved. Regardless of the specific environment, the City requires physical security requirements to be supported by all Business System Owners, Data Custodians, System Operators, and Users.

Administrative Rule
At a minimum, the following physical security measures and objectives must be implemented where applicable to protect City computing and network assets, and sensitive information:
• Mainframes, servers, network equipment, computer media containing sensitive data and other essential computer and network devices shall be stored in a secure location, such as a locked room, that protects them from unauthorized physical access, use, misuse, destruction or theft.
• Smoke/fire alarm and suppression systems are required for all data centers, server rooms and telecommunication closets to mitigate personnel harm and/or damage to City assets in the event of a fire.
• Temperature and ventilation control measures are required for all data centers and server rooms to protect City assets from preventable service disruptions or physical harm from environmental conditions.

• All mission critical data centers must employ emergency power control systems (backup generators or uninterruptible power supplies) to avoid disruptions and/or equipment/data harm due to power related failures.
• Inventory control measures such as inventory reports, asset tags or other identification markings for tracking are required per City accounting policy.
• All access to restricted areas, such as dedicated data centers, server rooms, and telecommunications closets, by unauthorized individuals must be conducted with an authorized City employee escort at all times.
• Access keys and key codes to restricted areas must be limited to only those individuals needing entry to fulfill their job responsibilities. Records of individuals' assigned access must be maintained.
• All specific tools, systems, or procedures implemented to meet physical security requirements must be selected on the basis of importance to safety, security and compliance with City policies and standards.
All City employees must be responsible to secure information assets in their care and possession and immediately report any loss or theft of such assets to their management and the Bureau of Technology Services. Additionally, all City employees must be aware of unauthorized individuals (e.g. maintenance, public and others visiting, delivery personnel, vendors, etc) and be prepared to challenge individuals entering data centers or other restricted areas.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.13 - Intrusion Detection - Printable Version

INTRUSION DETECTION
Administrative Rule Adopted by Council
ARC-BTS-2.13

Purpose
Intrusion detection plays an important role in implementing and enforcing the City's information security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

Intrusion detection provides two important functions in protecting information resources:
• Feedback: Information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
• Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.
The City Intrusion Detection Policy applies to all individuals that are responsible for the installation of new information systems, the operations of existing information systems, and individuals charged with information system security.

Administrative Rule

• Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.

• Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.

• Audit logging of any firewalls and other network perimeter access control system must be enabled.

• Audit logs from the perimeter access control systems must be monitored and reviewed by the system operators.

• System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.

• Audit logs for servers and hosts on the internal, protected, network must be reviewed by the system operators.

• System operators will furnish any audit logs to the Information Security Office upon request.

• Audit log review, in conjunction with event correlation software, may be delegated.

• Host based and network based intrusion tools must be checked on a routine basis when and where implemented.

• All trouble reports should be reviewed for symptoms that might indicate intrusive activity.

• All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the BTS Rule 2.08 INCIDENT REPORTING & RESPONSE.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.14 - Security Audits - Printable Version

SECURITY AUDITS
Administrative Rule Adopted by Council
ARC-BTS-2.14

Purpose
This policy outlines the authority for employees of the City's Information Security Office, in cooperation with BTS Operations, to conduct security audits on information systems at the City.

Audits may be conducted to:
• Ensure integrity, confidentiality and availability of information and resources
• Investigate possible security incidents and to ensure compliance to City security policies
• Monitor user or system activity where appropriate.

This policy covers all computing and communication devices owned or operated by the City. This policy also covers any computing and communications devices that are present on City owned premises or connect to the City network, but which may not be owned or operated by the City.

Administrative Rule
When requested, and for the purpose of performing an audit, necessary access will be provided to members of the City's Information Security Office and appropriate BTS Operations personnel. This policy does not supersede the requirement that the City auditor or other appropriate Bureau Directors approve access to the information, such as when it is restricted by law or State/Federal requirement.

This access may include:
• User level and/or system level access to any computing or communications device.
• Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on City equipment or premises.
• Access to work areas (data centers, computer rooms, telephone closets, labs, offices, cubicles, storage areas, etc.).
• Access to interactively monitor and log traffic on City networks.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.15 - Encryption - Printable Version

ENCRYPTION
Administrative Rule Adopted by Council
ARC-BTS-2.15

Purpose
Encryption technologies are used to prevent unauthorized individuals from reading or altering confidential or sensitive data stored on City systems or transmitted across City and public networks.

The purpose of this policy is to provide guidance as for where encryption technologies are to be implemented and limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that State and Federal regulations are observed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Administrative Rule

Applicability
Approved encryption techniques for the storage and transmission of information shall be implemented based on security risk management decisions which will be at the discretion of the CTO or delegate in consultation with the Information Security Manager and Business System Owner unless expressly required by legal regulation, statute or contractual obligation.

In general, the following types of sensitive or confidential data may be subject to the City's Encryption Policy:
• Criminal justice data when transmitted across public networks or any private network that is shared with non-criminal justice users
• User or application level credentials (account names & passwords)
• Credit card account numbers
• Data, when used together, results in a high risk for identity theft such as name, address, social security number & date of birth
• Electronic protected health information (ePHI) such as health benefit data covered under HIPAA privacy regulations
• Any 802.11 wireless or Remote Network Access communications when used to connect to the City's internal networks
• Confidential data stored on portable/mobile computing devices such as Laptops, PDA's and USB Thumb Drives which have a greater likelihood of loss or theft
Note: This is not a complete list and is provided to give general guidance on commonly used confidential/sensitive data subject to higher levels of protection. Please contact BTS for appropriate classification of data and to help determine if approved encryption is required.

Encryption Standards
Proven, standard algorithms such as 3DES, AES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the CTO or delegate, in consultation with the Information Security Manager (ISM).

City encryption key length requirements will be reviewed periodically and upgraded as technology allows.

Export Restrictions
Be aware that the export of encryption technologies is restricted by the U.S. Government.

Additional Considerations
Where networks and systems are under legal regulations such as Criminal Justice Information Systems (CJIS) Policy, there may be additional encryption requirements above and beyond the City's encryption policy.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-2.16 - Firewall Security and Management - Printable Version

FIREWALL SECURITY AND MANAGEMENT
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.16

Purpose

This policy describes the methods and responsibilities for securing the City internal network and data. Specifically, this policy outlines the standards and authority for managing the City's perimeter defense equipment known as firewalls.

Administrative Rule

The Information Security Office is responsible for developing all policies, standards and configurations for the implementation and use of firewalls within the City.

These policies and standards include but are not limited to:

- A stateful packet inspection firewall is required at each Internet connection.
- A stateful packet inspection firewall is required between any Demilitarized Zone (DMZ) and the City's internal network
- A stateful packet inspection firewall shall reside between the Internet and any City system or device.

Written justification is required to provide a connection through a firewall for any protocols other than HTTP, HTTPS, and SSH. Data owners shall submit written documentation for any other network protocols needed to conduct their business. This documentation shall include the business reasons for these protocols and the end date for this business need. The Information Security Office approves any requests for additional protocols and maintains all documentation on the business need for these protocols. All protocols from external and/or untrusted networks are not permitted without this written justification.

Firewall rules shall be reviewed by the Information Security Office at least once every six months to ensure the rules accuracy and continued necessity.

History

Adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 5, 2009.

BTS-2.17 - Payment Card Security Standards - Printable Version

PAYMENT CARD SECURITY STANDARDS
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.17

Purpose

The City collects payments using payment cards (credit and debit cards) for a variety of purposes. The payment cardholder association (Visa, Mastercard, American Express) requires that the City abide by specific information security standards, known as Payment Card Industry- Data Security Standard (PCI-DSS) in order to be permitted process electronic payments using various payment cards.

This section outlines specific PCI-DSS requirements related to the payment card process environment used for the City. The payment card environment includes any City systems and network that transmit, store, or process payment cardholder data. According to the PCI-DSS Security Standards Council, payment cardholder data is, at a minimum, the sixteen digit primary account number. Cardholder data may also appear in the form of the sixteen digit primary account number plus any of the following: cardholder name, expiration date, or service code.

Administrative Rule

The City shall abide by all aspects of the current PCI-DSS standard, as set forth by the PCI Security Standards Council (www.pcisecuritystandards.org). PCI-DSS include a variety of general and overarching information security standards that are addressed in other sections of the BTS Administrative Rules; however additional PCI-DSS specific standards are necessary in order for the City to achieve and maintain compliance with PCI-DSS. These standards include but are not limited to:

Encryption of Data

- All payment cardholder data shall be encrypted when transmitted over a public network such as the Internet or the City's internal network. Payment cardholder data is, at a minimum, the sixteen digit primary account number. Cardholder data may also appear in the form of the sixteen digit primary account number plus any of the following: cardholder name, expiration date, or service code.

- Only necessary data and protocols shall be allowed for payment card transactions. All other traffic or protocols are explicitly denied in the payment card environment.

Encryption Key Management

- Knowledge of encryption keys used in the payment card environment shall be restricted to the fewest number of custodians necessary and be based on business need.

- Encryption key custodians are the only personnel authorized to create, distribute, or maintain payment card environment encryption keys.

- Encryption keys must be changed at least annually. The keys may be changed more regularly as necessary and/or as recommended by the associated application.

- All compromised encryption keys must be replaced immediately.

- All encryption keys must be created with the use of strong passphrases in accordance with BTS Administrative Rule 2.05.

- Encryption keys must be strong keys. Strong keys are that meet the minimum recommended key size of comparable strengths recommendations in National Institute of Standards (NIST) Special Publication 800-57, March, 2007. (http://csrc.nist.gov/publications/).

- Encryption keys must not be stored or distributed in clear text. All keys must be encrypted with a key-encryption key.

- Encryption keys should be maintained under a split knowledge and dual control regime.

- Encryption key custodians must sign a key custodian form that recognizes and accepts all key-custodian responsibilities as listed above.

Authentication

- Shared passwords utilized to access any payment card systems or network are prohibited.

Monitoring

- All transaction and activity logs from relevant systems within the cardholder environment shall be reviewed daily.

- Logs from these systems shall be retained for one year from their creation date.

- Logs include, but are not limited to, user identification, type of event, date and time, success or failure indication, origination of event, identity or system component of affected data, or resources.

- Information Security personnel provide 24 X 7 incident response and monitoring coverage for any evidence of unauthorized activity. This coverage shall be manifested in the form of always available communications tools, such as email alerts, that provide readily available information on the status of secure transmission, storage, or processing of payment card data.

Physical Access

- Obsolete paper copies of payment cardholder data must be cross-cut, shredded, incinerated, or pulped once they are no longer needed.

- Physical storage of paper copies of payment cardholder data must be done in a secure environment which includes locked containers.

- End-of-life electronic media used to store payment cardholder data must be purged, degaussed or otherwise destroyed so that cardholder data cannot be reconstructed.

- No payment cardholder data shall be transmitted via end-user messaging technologies including, but not limited, to email and/or instant messaging.

- Storage of all payment card data will be kept only to complete the payment transaction and will not be stored longer than business needs require. At no time after card authorization, under any circumstance, will the City store any information from the card magnetic track, to include Card Validation Value/ Card Validation Code (CVV)/(CVC), CVV2/CVC2, and Personal Identification Number (PIN) block data.

- Account Numbers will be masked when displayed. At any time, the first six and last four digits will be the maximum number of digits to be displayed.

- All media with cardholder data will be audited on a quarterly basis to ensure that stored classified data does not exceed business retention requirements and the retention schedule is adhered to.

System Development Life Cycle

- Software patches to payment card software must be properly tested before being deployed into production.
- Test/development environments are separate from the production environment, with access controls in place to enforce such separation.
- Test/development personnel must employ separation of duties from production environment personnel.
- Production data (such as active primary account numbers) are not used for testing and development, or are sanitized before use.
- Test cardholder data and accounts are removed before a production system becomes active.
- Custom application accounts, usernames and/or passwords are removed before a payment card system is placed into production.
- Custom software code for payment card processing must be reviewed prior to release to production in order to identify any potential coding vulnerabilities.
- Software code reviews must be conducted by an individual other than the code author.
- Development of all web applications should be based on secure coding guidelines such as the Open Web Application Security Project Guidelines (OWASP) and PCI-DSS Requirement 6.5.

General Payment Card Security

- The City shall conduct an annual risk assessment of its payment card environment. Involved parties shall be the Data Custodian, and the Information Security Office.
- The Information Security Office shall conduct an annual review of its security policy as it relates to the payment card environment and update the policy whenever changes in the cardholder environment or PCI rules necessitate a change.
- Only devices authorized by Information Security shall connect to any payment card systems.
- All modems must automatically disconnect after 15 minutes of inactivity
- No cardholder data may be stored or copied onto any personal computers or other media not used as part of a centralized backup data solution.
- All payment card systems and/or devices that transmit, store, or process cardholder data must be properly labeled with the current owner, contact information, and purpose of the system or device.
- A current list of all systems or devices that transmit, store, or process cardholder data shall be maintained by the Data Custodian and Information Security Office.
- The physical locations for all payment card systems or devices shall be reviewed and approved by the Information Security Office.

History

Adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 5, 2009.

BTS-3.01 - E-Government Services - Printable Version

E-GOVERNMENT SERVICES
Administrative Rule Adopted by Council
ARC-BTS-3.01

Purpose
E-Government is a process by which the City delivers information and services electronically. It allows citizens and businesses easy access to government and streamlined business processes. E-Government interactions are often categorized in terms of citizen or business to government, government to citizen or business, and government to government. Government to government can also include providing employees easy access to electronic information and processes which improve their productivity. E-Government will evolve from a basic web presence to a fully connected integrated digital environment where citizens, government and employees can seamlessly interact with the City 24 hours a day, 7 days a week.

Council Resolutions 35413, 36109, and 36170 provide the foundation for the City's pursuit of E-Government.

This BTS Administrative Rule addresses development and ongoing management of City E-Government Services to achieve these primary goals:

- The development of a single City web portal.
- The development of a single identity and sign on system for both Citizens and staff.
- Process all secure E-Commerce transactions.

Web Content Management and Publishing
The Bureau of Technology Services provides the infrastructure, software and basic presentation and navigation format for the City web presence. Bureaus shall use the PortlandOnline Content Management System (CMS), to manage all Internet web content. PortlandOnline shall serve as the portal to access all customer facing City web applications in order to achieve the objective of Council Resolution 35413.

All news, policy and project posting shall comply with Council Resolution 36109, requiring inclusion on the news page of PortlandOnline.

All notification of meetings for the general public shall comply with Council Resolution 36170, requiring inclusion in the calendar application within PortlandOnline.

To maintain the coherence of the City of Portland web presence, and to leverage the investments in the internet platform, all projects, consulting, equipment, and software acquisition relating to web content presentation and web applications will be subject to the project review and approval by the CTO or designee.

As the PortlandOnline CMS can securely integrate information traditionally separated as an Intranet, restricting such information to employees or employee groups, while providing unified access to both "Internet" and "Intranet" content and the efficiency advantages of the CMS for publication and simplified infrastructure, Bureaus are encouraged to migrate Intranet content to the CMS as soon as practical.

E-Services
E-Services such as permitting, billing, licensing etc. will be made available using an Enterprise strategy and architecture. Any Bureau that is looking to provide an E-Service must coordinate with the Bureau of Technology Services at the earliest opportunity.

To leverage the security and integration investments in the City's Web platform, any and all projects, consulting requests, equipment and software acquisition requests relating to E-Service delivery will be subject to review and approval by the CTO or designee.

User Authentication
All online services that require user authentication will utilize the standard PortlandOnline Single Sign-On system. Any online service that requires storing user account information for security, enhanced service or future correspondence will be stored and managed in the central City directory. With the unified authentication system, Bureaus will retain the ability to establish the criteria and process to authorize users to access their Bureau specific applications.

E-Commerce
When City Bureaus have electronic commerce service applications that allow electronic receipt of electronic check or credit card transactions such as Visa, or Master Card over the web, the electronic receipts approval requests will be routed to the centralized Payment Processing Gateway (PPG) for approval or disapproval by the City's merchant services provider. PPG is a City developed electronic payment processing web service and connection mechanism to route credit card receipts to the City's payment processing provider, with integration to support the reconciliation process. Note: Discover and American Express cards are not allowed for electronic payment unless specific approval has been received from the Treasury Division.

All E-Commerce transactions must be approved and comply with standards and polices set by the Treasury Division.

Any acquisition or implementation of an alternative electronic receipt approval process must be approved by the CTO and City Treasurer. The Bureau of Technology will have responsibility for the technical assessment of the compatibility of any proposed alternatives to PPG and will render a final decision once that assessment has been completed. The Treasury Division is responsible for the contract administration of the City Credit Card processor contract and coordination of City Bureaus utilization of that contract.

BTS shall be responsible for periodic review of the security mechanisms that support E-Commerce.

Web Services and Infrastructure
All public and private callable "Web Service" functions must be coordinated with the Bureau of Technology Services to comply with both architecture and security standards. BTS will be responsible for implementing and managing all necessary IT infrastructure related to delivering web based services and applications. This includes but is not limited to hardware, software, networks and security.

Domain Names
The City of Portland , consistent with adopted policy, has transitioned and branded into the new domain name www.portlandonline.com. While the www.ci.portland.or.us domain name will remain in effect, www.portlandonline.com is the official City web address. Bureaus are expected to have completed their transitions to PortlandOnline by December 31, 2005.

The Bureau of Technology Services has ownership of the portlandonline.com domain and makes it available to agencies that are launching applications, even if not part of the PortlandOnline technology platform.

Bureaus will not be permitted to insert bureau identifiers between the www and portlandonline.com to create a sub-domain address such as www.bts.portlandonline.com.

Where Bureau identifiers are necessary, they will follow a virgule after the .com to form an address similar to www.portlandonline.com/bts. In this example the letters “bts” act as the abbreviation for the "Bureau of Technology Services". Readily identifiable character combinations should be used to identify Bureau service areas. The use of new alternative addresses for access to City websites requires the approval of the CTO and the Commissioner-in-charge of the Bureau
and should meet at least one of the following criteria:

- The website is a special purpose website with an audience with limited expected overlap with the PortlandOnline users community

- The website is a special purpose website under the control of an intergovernmental or public/private partnership where branding the City’s leadership will lead to partnership relationship problems; unless essential to sustaining the partnership, this exception should not be used if the City’s contribution is significant and in support of a Council priority objective.

All domain name registration and management will be the responsibility of the Bureau of Technology Services.

All new and renewal domain registration requests must be approved by the CTO.

Archived Records
Bureaus and Offices will maintain an official archive of version records of all appropriate archival material posted on the web site. Bureaus will remove and archive information according the City Auditor policies and procedures.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-3.02 - Web Publishing - Printable Version

WEB PUBLISHING
Administrative Rule Adopted by Council
ARC-BTS-3.02

Purpose
The purpose of web publishing for the City and its Bureaus is to improve two-way communication with City officials and staff, provide efficient access to information about City services and programs, and offer a cost-effective alternative for conducting business with the City. City and Bureau web pages are established as a means for the City to provide information to the public.

City Web Sites
The Bureau of Technology Services manages the infrastructure and basic presentation and navigation format for the City Internet and Intranet. PortlandOnline functions as the City Internet and Intranet system. Bureaus shall use the standard formats and navigation structure for all bureau specific Intranet and Internet sites in accordance with PortlandOnline CMS "Best Practices and Standards", to provide a common look and feel to the City's Web presence, while supporting individual bureau identity. See http://www.portlandonline.com/support.

City and Bureau Web sites will be designed and maintained to achieve these goals:
• The cumulative City web presence shall form a coherent, cohesive whole;
• Meet the information and business needs of the different user audiences and visitors to the City's Web presence;
• Benefit Portland residents, the City of Portland , and Internet users worldwide.
• Use graphics and page formatting to complement the text or aid in navigation;
• Meet federal Americans with Disabilities Act web access requirements
Only personnel authorized by the City may make changes to City sites.

City Bureaus are authorized to publish information directly related to their Bureaus. Bureau Managers shall approve all such Web content and ensure they comply with existing policies and practices with regard to official City or Bureau communication, including review processes for correspondence and published materials. Individual bureaus will be responsible for assigning appropriate security roles that control read, write, and modify permissions with respect to their content to enable personalized delivery of information to citizens, and bureau and City staff.

Bureaus shall limit the content of their Web pages to their area of responsibility. If Bureau responsibilities overlap or are shared, the Bureaus should confer to ensure to avoid duplication and to ensure the best integration, accuracy and timeliness of information. Bureaus shall ensure that material that is located on another City web page is not duplicated. Rather, they shall provide a link to the authoritative source.

All material that is available on the City's Internet site shall also be accessible by City staff who only have access to the City's Intranet; utilizing the PortlandOnline CMS for Intranet content is the most efficient way to ensure that City staff have access to the entire range of content.

Web Content and Linkage
City boards or commissions shall coordinate Web publishing with their sponsoring City agency.

The City may from time to time establish hyperlinks to non-City web sites (typically those established by community, public-interest or other similar entities) when the City determines

that a linked site will enhance or supplement information the City is providing on its web pages about the City's programs, policies, mission and objectives. Such links may be established by City staff only where the above criteria are met, and the linked sites are consistent with City code and policies.

All City web sites must include the most current Disclaimer and Privacy Statement from the City Attorney's office.

All City web sites must include a contact link to a Webmaster for the site.

History
Originally published as PPD number ARC-BIT-1.09, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-3.02.

BTS-3.03 - Web Infrastructure - Printable Version

WEB INFRASTRUCTURE
Administrative Rule Adopted by Council
ARC-BTS-3.03

Purpose
The purpose of this policy is to support the development and use of a consolidated and consistent web infrastructure to support secure and efficient EGovernment business processes.

Secure Functionality
The Bureau of Technology Services shall maintain a standardized and secure EGovernment infrastructure and environment. This includes providing common service modules that all entities shall use to implement digital signatures, electronic payments and similar online tasks.

BTS is the City of Portland 's sole authority for the security infrastructure for providing electronic certificates, digital signatures and encryption mechanisms.

Online Payment Processing
Upon its availability, all City financial transactions will be processed through a single transaction tool that will be integrated with the City's financial management system and/or data repository system.

PortlandOnline
The E-Government initiative is centered on a web portal called **PortlandOnline**.

PortlandOnline provides a single portal to reach all existing web services provided by Bureaus today as well as features which will enhance service and information delivery options for users and service providers.

Those features are supported at the corporate and Bureau levels, through standardized components, applications, enterprise-wide infrastructure and business processes.

Stakeholder Involvement
The CTO will use an appropriate mechanism(s) to facilitate stakeholder collaboration in the transformation of business processes to support Portland Online. The scope of such collaboration may include, but is not limited to:
• Use of existing, established workgroups or forums;
• Establishment of new workgroups comprised of relevant personnel;
• Establishment of technical committees to provide expertise in the transformation of the business process, including but not limited to, the preparation of technical standards and specifications, and/or assisting in the preparation of data or analysis for a business case analysis of proposed alternatives.
Stakeholders may include City managers, staff, and/or representatives from the private sector, or the general public.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-4.01 - Software Application Life Cycle - Printable Version

SOFTWARE APPLICATION LIFE CYCLE
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-4.01

Purpose

The City shall adopt a consistent, cost effective, approach to application services to fully meet the City's business requirements. This approach will include all aspects of project management and software development lifecycles including the initial request for service, the documentation developed as a result of the request, the Citywide Application Evaluation Review and the City Systems Development Methodology. These processes were developed pursuant to Council Ordinance 175331, adopting recommendations on the Administrative Services Review.

Application services include requests to modify, enhance or develop GIS, Web, client or server based applications. Application services also include any requests that might result in the purchase and implementation of a commercially available application system.

The purpose of this policy is to standardize the application life cycle to:

- Use a common, simplified, scalable method to develop, purchase and implement applications.
- Ensure a careful review to make best use of City resources.
- Set realistic expectations with customers regarding the budget, timelines and resources to develop, implement and maintain applications.
- Maintain an enterprise citywide systems perspective.

In addition, Council Resolution 36454 directed all City bureaus to continue to collaborate on the Enterprise Business Solution (EBS) project and to give the project high priority. Council also directed bureaus to limit requests for new information technology projects during the implementation of the EBS project, and to request only those projects that do not interface with EBS and are of the highest priority.

Administrative Rule

All application service requests - outside of a production failure or an emergency as determined by the CTO or designee - shall be submitted using the Project and Services Request Process. This procedure is described on the BTS website located at http://www.portlandonline.com/bts.

Project requests will proceed according to the BTS project management process including, but not limited to, the following high level steps:

- Bureaus submit requests via the City Project and Service Request process, by preparing and submitting a BTS Project Intake Document (PID).
- Requests for new applications will be evaluated by the BTS Strategic Technology Team.
- Bureaus will use an IT project management process as specified by BTS.
- Software development and purchases will be done according to the City Systems Development Methodology and City IT standards.

In order to facilitate the processes above:

• All project and service request for applications services will be submitted to the BTS Request Tracking system and follow the BTS project and service request process outlined on the BTS website.

• All applications shall be documented in the City's Application Evaluation database. All proposed application development projects shall be checked against the Application Development Clearinghouse to ensure that no comparable tools already exist. Relevant tools/applications already in existence shall be examined for applicability to the task at hand. This process is described on the BTS website.

• The City Systems Development Methodology will be used to define the activities to be carried out in a project, to introduce consistency among the many projects, to insure appropriate communications occur with all of the stakeholders and to provide checkpoints for management control and for "go/no go" decisions. The Systems Development Methodology is on the BTS Intranet site.

• Applications to be purchased or developed shall conform to applicable City standards. City IT Standards are in the BTS website Customer Service area.

Additional Review
During the implementation of the EBS project, bureau requests for new information technology projects will receive additional review and prioritization:

The BTS Strategic Technology Team will review the project to see if it has scope related to the City's financial, procurement and human resources/payroll systems and whether it can be added to the BTS workload without affecting the schedules for the other large-scale City IT projects.

If the team determines that the project scope does not relate to those systems and would not delay the schedules for other large-scale IT projects, the team will work directly with the requesting bureau to complete the work. If the team determines that the project scope does relate to those systems or may cause delays to other large-scale IT projects, and the Chief Technology Officer concurs, the team will forward the PID to the Chief Administrative Officer for review by the Office of Management and Finance (OMF) Advisory Committee.

Responsibility

Bureau Business Representatives
The Bureau Business Representative (BBR), identified for each Bureau, will document requests for services in collaboration with bureau personnel. The BBR will use the BTS Request Tracking system to maintain lists of bureau project and service requests for application services. BBRs will work with bureau representatives to ensure compliance with all BTS Administrative Rules and Standards.

All applications shall be documented in the City's Application Development Clearinghouse database. This database shall be maintained by BTS and bureau staff as appropriate.

The BBR will work with each bureau to identify a fiscal year work plan for application development services provided through a Service Level Agreement with BTS. New projects shall be prioritized by the bureau.

BTS will promote and facilitate partnerships among bureaus for application development.

Office of Management and Finance Advisory Committee
For those projects that require review by the OMF Advisory Committee:

The OMF Advisory Committee will review the PID and its assigned priority by the requesting bureau, and determine a citywide relative priority. The Chief Administrative Officer will invite the requesting bureau to participate in the Advisory Committee meeting to discuss the project.
• If the committee determines that the project is medium or low priority, the PID will be returned to the requesting bureau, the project will be put on hold and the Chief Administrative Officer will notify appropriate project offices.
• If the committee determines that the project is critical or high priority, the Chief Administrative Officer will notify the requesting bureau and forward the PID to either the strategic tech team for follow up or the EBS project management office for additional review. The EBS office will assign it to the appropriate EBS project lead.

EBS Project Review
The EBS project team lead will create an EBS project change request. The project lead will enter the request into the solution management software and make appropriate notifications.

The project lead will assess and validate the impact of the proposed project on system design, project scope, schedule and budget, and will forward the analysis to the EBS project management office for review.

If the EBS project management office determines that the proposed project has no impact on system design, scope, schedule, resources or budget, the office will:
• Notify the EBS Change Control Board.
• Notify the OMF Advisory Committee and requesting bureau that either a) the project is included or will be included in the system design or b) the project can proceed without a change to the EBS project.
• Forward the project change request to the EBS project team lead, for inclusion in the EBS (if not already included).
• Make other appropriate notifications.

If the EBS project management office determines that the proposed project does impact system design, scope, schedule, resources or budget, the office will:
• Forward the project change request impact analysis to the EBS Change Control Board for review.
• Notify the OMF Advisory Committee and requesting bureau.
• Make other appropriate notifications.

The EBS Change Control Board will review the request and recommend approval, deferral or rejection to the EBS Executive Steering Committee.

EBS Executive Steering Committee
The EBS Executive Steering Committee will review the project change request impact analysis; approve, defer or reject the project request; and return the request to the EBS project management office.

If approved, the EBS project management office will:
• Notify the OMF Advisory Committee and requesting bureau.
• Prepare the necessary scope changes, contract amendments and/or Council ordinances.
• Make other appropriate notifications.

If deferred or rejected:
• Return the PID to the requesting bureau.
• Notify the OMF Advisory Committee.
• Make other appropriate notifications.

Administrative Rule History

Originally published as PPD number ARC-BIT-2.08, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999, passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-4.01.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 7, 2007.

BTS-4.02 - Shared Data - Printable Version

SHARED DATA
Administrative Rule Adopted by Council
ARC-BTS-4.02

Purpose
Access to accurate, consistent data is critical for the operational performance of the City's Bureaus and Offices.

The purpose of this policy is to define the methods and responsibilities for storing and managing common, shared data to minimize the likelihood of compromises to data integrity and confidentiality while providing for efficient and cost effective services.

Administrative Rule
The City of Portland shall establish and maintain a repository for data (in single or multiple locations as appropriate) or hub for all corporate data; data defined as "confidential" by applicable City Code, State statute, Federal laws or binding legal agreement may be stored separately or stored in a common repository provided appropriate safeguards are provided for this confidential data in the repository and in transit to and from the repository. SeeCity Code 6.04.130.

Responsibility
Bureaus shall work with BTS to achieve a long-term goal of reducing duplicate instances of shared data, to improve data integrity across the enterprise.

The Bureau of Technology Services shall be responsible for the maintenance of the corporate data repository or hub systems, as well as the appropriate data access tools for the City of Portland.

Business System Owners and Data Custodians are responsible for defining access privileges and classifying data appropriately as to its level of confidentiality. See BTS Rule 2.02 SECURITY ROLES & RESPONSIBILITIES.

System Operators are responsible for the internal procedures that ensure secure access to and protection of data stored in the business data repository system.

History
Originally published as PPD number ARC-BIT-2.09, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-4.02.

BTS-4.03 - Data Backup - Printable Version

DATA BACKUP
Administrative Rule Adopted by Council
ARC-BTS-4.03

Purpose
Data backup is a process that stores redundant copies of electronic files and data from hard disk to a separate storage environment, usually through the use of removable media, such as tape. The redundant copies of files are used or "recovered" when the original files are damaged or accidentally deleted. Any new files or files that have changed since the last backup are copied to the separate storage environment to assist in immediate restoration if data is lost.

Computer data obtained or generated while conducting City business are City property and represent a significant investment of time and financial resources.

The purpose of this policy is to define requirements and expectations with regards to Data Backup services provided by the Bureau of Technology Services (BTS)

Administrative Rule
BTS shall backup City data on systems or network storage devices according to the backup procedures developed by BTS personnel in support of requirements as defined by the Business System Owners and Data Custodians. Backup procedures will address the business needs of City's Bureaus and Offices and follow established standards. Deviation from the standard backup schedule, duration of historical data retention (such as required by public records archival rules or bureau specific needs), backup media and other established standards must be properly justified.

The backup of sensitive or confidential data shall be subject to BTS Rule 2.05: ENCRYPTION.

Backup media must be properly stored to protect electronic data from damage and/or theft. All backup media containing "full" copies of data must be stored at a secure off-site location unless an exception has been granted by the CTO. Under no circumstances shall backup media be stored at non-City facilities.

In general practice, personal desktop/laptop computers and portable computing devices are not supported by BTS backup services and therefore should not be used to store sensitive, confidential or critical data.

Please note that non-standard backup and retention schedules or backup of personal desktop/laptop computers or personal computing devices may be subject to additional BTS materials and service bill-back charges.

Responsibility

Bureau of Technology Services
BTS staff shall conduct regular backups of data systems as per industry best practices and in accordance with City business and legal requirements.

BTS staff shall maintain documentation of backup procedures including:
• Identification of individuals and alternates responsible for carrying out backup and restore tasks
• The frequency of backups and data retention schedules

• Identification of the location for the proper storage of backup media and methods for transport
• Identification of circumstances requiring review and/or modification of the procedure

Bureaus and Individual Users

Responsible for preserving work to a BTS supported and backed up network storage location. BTS will provide appropriate technology and training where necessary to accomplish related tasks.

Responsible for defining appropriate retention schedules in support of business need and legal requirements. Note: Records Retention and Disposition Schedules governing information technology are promulgated by the City Auditor's Office and can be found at http://www.portlandonline.com/auditor/

History

Originally published as PPD number ARC-BIT-2.10, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-4.03.

BTS-5.01 - Corporate Geographic Information System -
Printable Version

CORPORATE GEOGRAPHIC INFORMATION SYSTEM
Administrative Rule Adopted by Council
ARC-BTS-5.01

Purpose
The Corporate Geographic Information System (CGIS) supports both City customers and clients. Customers include the City's citizens, business partners and others who are governed and regulated by City Code, and who support City services through Portland 's system of fees and taxes. Clients are composed of City bureaus and divisions who serve Portland 's customers.

The primary focus of CGIS is to ensure the City leverages existing investments, eliminates redundancy, promotes standardization and consolidation and provides business efficiencies to the City using scalable enterprise GIS technologies.

The purpose of the CGIS policy is to define how the City will promote, use & support those technologies which improve customer service through improved response time, improved access to information and though the overall reduction of service costs.

Administrative Rule

Standard Software
The City has standardized on ESRI GIS software. Through the Corporate GIS program, an Enterprise License for software is maintained and is the sole conduit for Bureaus to obtain software and licenses for use of GIS software in the City.

Preexisting non-standard software will be considered for migration to the City standard at its next version upgrade. As new versions are targeted for migration, bureaus and CGIS will proactively plan to migrate to the City standard in the timeline identified by the migration planning process. This will ensure that the City continues to realize the financial benefits of the Enterprise License.

Bureaus will be required to maintain ESRI software version compatibility with the current BTS standard supported version. CGIS will assist in version upgrade planning, support and deployment. Bureaus will be responsible for maintaining current version compatibility on all bureau databases and bureau developed applications.

Software Installation, Use and Reporting

In order to comply with the ESRI Site License agreement, all ESRI software installations will be coordinated and reported to CGIS. Installations and uninstalls will be reported no later then 5 business days after the work has been completed.

All installations of ESRI desktop GIS software shall be deployed with the CGIS developed corporate extensions and software such as the CGIS Tool bar. The CGIS Tool bar is the standard toolset that facilitates access to HUB datasets and layers.

Data Publishing to the Hub
In order to eliminate and/or reduce duplication of data and to provide secure, accurate and up to date data to users, all data that will be used by more then the originating Bureau will be posted and made available on the Enterprise GIS Hub. In general, exporting and distributing

data directly to other Bureaus and end users is not permitted as this can create data integrity issues as well as unmanageable data dependencies.

Data Custodians are responsible for defining access requirements, update frequencies and metadata currency. Data Custodians work in conjunction with System Operators to ensure that “due care” is taken to properly protect sensitive data.

Metadata
CGIS supports a central online Metadata system. All Data Custodians will ensure that the central metadata repository is maintained and current at all times. Data that does not contain the minimum set of metadata as defined in the CGIS Metadata Standard is not to be distributed either internally or externally.

GIS Web Mapping Services
All public and private callable “GIS Web Mapping Service” functions are to be provided by the Bureau of Technology Services (BTS) to ensure compliance with both architecture and security standards.

BTS is responsible for implementing and managing all necessary IT infrastructure related to delivering web based GIS services and applications. This includes but is not limited to hardware, software, networks, support and security.

Disclaimer Statement
All printed and online maps will incorporate a standard disclaimer as defined in the “Corporate Spatial Data Distribution Standards” maintained by CGIS. See http://www.portlandonline.com/gis.

Data Distribution
In order to effectively and securely manage data distribution both internally and externally to customers and citizens, all distributed data will comply with the “Data Distribution and Use Agreement Polices”. See http://www.portlandonline.com/gis.

GIS Application Procurement, Development and Deployment
All development, deployment or purchase of GIS tools and applications will be coordinated with CGIS in accordance with BTS Rule 4.01: SOFTWARE APPLICATION LIFECYCLE.

Corporate Data
In order to efficiently maintain the Cities corporate data layers for all City users, CGIS is responsible for the maintenance and development of corporate datasets including: cadastre, centerline and the address model. Projects that rely on these or related datasets should be conducted with the involvement of CGIS to ensure compliance with City standards and policies such as the CGIS Addressing Guide.

Exceptions
Any exceptions to this policy must be must be approved by the Chief Technology Officer (CTO) or designee.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.

BTS-6.01 - Technology Definitions - Printable Version

TECHNOLOGY DEFINITIONS
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-6.01

Definitions

The following information and communications technology definitions and terms are used in the Bureau of Technology Services Administrative Rules and associated standards and guidelines.

These definitions are not part of the binding BTS Administrative Rules.

802.11: A family of IEEE specifications for wireless local area networks.

802.1X: A standard developed by IEEE designed to enhance the security of both wired and wireless networks. 802.1X provides an authentication framework allowing a user or device to be authenticated by a central authority.

Access Control: Physical, procedural and/or electronic mechanism which ensures that only those who are authorized to view, update and/or delete data can access that data.

Access Point: Also know as a wireless base station. A hardware device that acts as a communication hub for users of a wireless device to connect to a wired local area network.

Algorithm: An unambiguous formula or set of rules for solving a problem in a finite number of steps. Algorithms for encryption are usually called Ciphers.

Analog Line: A communications line, such as a standard telephone line, that carries information in analog (continuously variable) form.

Analog Modem: Communications equipment which converts computer information/data, in the form of digital pulses to audio tones that can be carried over analog telephone lines.

Anonymous Access: A method which allows access to applications or systems without requiring user identification and password authentication.

Anti-Virus Software: A software program designed to identify and remove a known or potential computer virus, worm or trojan horse

Application: Software that performs a specific task or function, such as word-processing, creation of spreadsheets, generation of graphics, facilitating electronic mail, etc

Asset: A physical item, informational item, or capability required by an organization to maintain productivity. Examples include computing systems, communication systems and data.

Attachment: A file attached to an e-mail message.

Authentication: The assurance that a party to some computerized transaction is not an impostor. Authentication typically involves using a password, certificate, PIN, or other information that can be used to validate the identity over a computer network

Authorization: The process of giving someone permission to do or have something; a system administrator defines for the system which users are allowed access to the system and what privileges are assigned.

Availability: The assurance that a computer system is accessible by authorized users whenever needed, as pre-defined, or as established through a Service Level Agreement.

Backup: The activity of copying electronic data so that it will be preserved in case of equipment failure, accidental or malicious loss or other catastrophe.

Breach: The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Business System Owners: Individuals within the City who are ultimately accountable for the budget, management, and use of one or more electronic information systems or electronic applications that are associated with the City of Portland (e.g. Bureau Directors). Electronic information systems cover a wide range of business requirements and 'ownership'. They may be single-purpose/single-bureau business applications as well as multi-purpose/multi-bureau business applications. Business applications may also be 'enterprise' applications that serve the common functional requirements of all City bureaus and offices (e.g. various administrative information systems).

Change Management: Process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.

Cipher: A method that encrypts or disguises text. Ciphers replace the message letters with other letters, numbers or symbols, as in substitution, or move around the individual letters of the plaintext, as in transposition – or a combination of both.

Common Criteria: A comprehensive specification that first defines the targeted environment and then specifies the security requirements necessary to counter threats inherent in that environment.

Compliance: A user, device, computing system, network element or operating system is in compliance with a policy when it implements and adheres to all functional aspects explicitly stated as required in that policy.

Compromise: Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of data is suspected.

Confidentiality: An attribute of information. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial.

Cost-effective: To deliver desired results in beneficial financial terms.

Credential: A general term for privilege attribute data that has been certified by a trusted privilege certification authority

Cracking: The process of overcoming a security measure. Also commonly referred to as Hacking.

Criticality: A relative measure of the consequence of a particular failure mode and its frequency of occurrence.

Cryptosystem: A system used for encrypting and decrypting data. Usually involves an algorithm for combining the original data (plaintext) with one or more keys - numbers or strings of characters known only to the sender and recipient - into cipher text.

Database: A shared collection of logically related data, designed to meet the information needs of multiple users in an organization.

Data Custodians: Data Custodians are business experts who have been officially designated by the Bureau of Technology Services and/or Bureau Business System Owners as accountable for the definition of specific business requirements regarding protection of the confidentiality of specific data that is transmitted, used, stored, and maintained on City of Portland information systems. Data Custodians help translate the business requirements into appropriate system security procedures that are aligned with the City of Portland Information System Security Policy.

Degaussing: Also called "disk degaussing." Process or technique that demagnetizes the disk such that all data stored on the disk is permanently destroyed.

DMZ: Short for demilitarized zone which is an internal network typically used exclusively for servers that are accessed by external clients on the Internet, such as web servers. Placing these public access servers on a separate isolated network, provides an extra measure of security for internal networks

DNS: Also know as a Domain Name System (or Service) which translates alphabetic domain names into numeric IP addresses.

Download: Transferring data (usually a file) from another computer to the computer you are using.

Dual Control: A procedure whereby the active involvement of two people is required to complete a specified process.

E-Commerce: A way of supporting real-time business transactions via the internet.

E-Government: The process by which the City delivers information and services electronically. It allows citizens and businesses easy access to government information and streamlined business processes.

Encryption: The transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it was not intended, including those who can see the encrypted data.

End-of-Life: A status where data or devices has exceeded its useful life and should be eliminated or replaced.

Entitlement: Any of the benefits to which one is entitled, or to which one is given a right, by meeting specific eligibility requirements.

Electronic Protected Health Information (ePHI): Individually identifiable electronic health information that is stored and/or transmitted that relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual.

Ethernet: The common method of networking computers in a LAN, or Local Area Network.

Extranet: A private network that uses internet protocols and the public telecommunications system to securely share part of a business's information or operations with suppliers, vendors, partners, customers or other businesses.

Firewall: A combination of hardware and software that secures access to and from a network based on rules.

Firewall Rule: A set of logical statements within a firewall that permit or deny internal and external network traffic to flow through it to various destinations and/or devices.

Frame Relay: Standard packet-switched protocol for transmission of voice and data that creates "virtual" dedicated circuits. These are less expensive than dedicated circuits.

Gateway: A hardware and/or software set-up that translates between two dissimilar protocols

Governance: The authority for defining policy, providing leadership, and managing and coordinating the procedures and resources that ensure the security of information systems

Hash Number: Also called "hash function" or hashing, used extensively in many encryption algorithms. Hashing transforms a string of characters usually into a shorter, fixed-length value or key.

HIPAA: Short for the Health Insurance Portability and Accountability Act of 1996**.**

Incident Response: The ability to respond appropriately and completely to any incidents, situational compromises, or threats from any source at anytime.

Information System: The network or combinations of all computing equipment, telecommunication or other communication or information processing devices and channels used within an organization.

Infrastructure: The computer and communication hardware, software, databases, people, and policies supporting the enterprise's information management functions.

Integrity: The condition of data or a system, in which that data or system remains intact, unaltered, and hence reliable.

Internet: The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's.

Intranet: Contrary to the public Internet, an intranet is a private network inside a company or organization.

Intrusion Detection: A security management system and or process that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attack from outside the organization) and misuse (attacks from within the organization).

IPSEC: Short for Internet Protocol Security. Security functions (authentication and encryption) implemented at the IP level of the protocol stack.

ISDN Line: Also know as an Integrated Services Digital Network. A digital telephony scheme that allows a user to connect to the Internet over standard phone lines at speeds higher than a 56K modem allows.

Key: A piece of information that determines the functional output of a cryptographic algorithm or cipher. Without a key the algorithm would have no result. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption.

Language: A formal language with a particular set of 'grammatical' rules and guidelines used in writing a computer program or software.

LDAP: An acronym for Lightweight Directory Access Protocol which is a network protocol designed to help users extract information from a hierarchical directory in a network, whether on the Internet or on a corporate intranet.

Mobile Device: Any computing or communications device intended to frequently move location while maintaining function and operation.

Modem: A device that allows computers to communicate with each other over telephone lines or other delivery systems by changing digital signals to telephone signals for transmission and then back to digital signals.

Malware: Short for malicious software and is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms and trojan horses.

MAC Address: Short for media access control address; the unique physical address of each device's network interface card

Memory: The space used by a computer to hold the program that is currently running, along with the data it needs.

Mitigate: The action of reducing or minimizing the severity of the impact or likelihood of a risk or an event.

Multi-user: A system or program designed to accommodate simultaneous use by multiple users,

Need-to-Know: An administrative action certifying that a given individual requires access to specified private information in order to perform his or her assigned duties.

Network: A collection of two or more computer or communication systems interconnected by telephone lines, communications cables, satellite links, radio, and/or other communication techniques.

Network Interface Card: An expansion board you insert into a computer so the computer can be connected to a network.

Non-repudiation: A mutually agreed process, secured evidence, or other method of operation which provides for proof of receipt or protection from denial of an electronic transaction or other activity.

Operating System: The foundation software of a machine; that which schedules tasks, allocates storage, and presents a default interface to the user between applications.

Ownership: The term that signifies decision-making authority and accountability for a given span of control.

Password Protection: The ability to protect a system, data or object using a password

Pass Phrase: The word or phrase that protects private key files. It prevents unauthorized users from encrypting them.

Patch: A piece of code added to software in order to fix a vulnerability or bug, especially as a temporary correction between software releases.

PDA: Short for personal digital assistant, a small handheld device that combines one or more computing and/or communications functions such as email, calendar, internet and phone.

Penetration Testing: A security evaluation performance wherein practitioners attempt to gain access to a system despite security features.

Physical Security: The component of information security that results from all physical measures necessary to safeguard equipment and data, from access by unauthorized persons or electrical or environmental (fire, smoke, temperature, etc) damage.

Portal: A starting point web page with a hierarchical, topical directory, a search window, and added features like news headlines applications and links to informative and collaborative services and applications.

Port Scanning: A program that attempts to learn about the weaknesses of a computer or network device by repeatedly probing it with requests for information.

Principle of Least Privilege: An operations principle that requires access privileges for any user to be limited to only what they need to have (nothing in addition) to be able to complete their assigned duties or functions.

Principle of Separation of Duties: An operations principle that requires that whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse or other harm.

Privacy: The protection of sensitive data and personal information from unintentional and intentional attacks and disclosure.

Privilege: A user's right to perform a specific task on an information system. Privileges are assigned by administrators to individual users or groups of users as part of the security settings for the computer.

Proprietary: Refers to a technological design or architecture whose configuration is unavailable to the public and may not be duplicated without permission from the designer or architect.

Protocol: Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data.

Public Network: A network established and operated by a telecommunications provider, for specific purpose of providing data transmission services for the public. Examples of public networks in scope of the PCI DSS include, but are
not limited to, the Internet, wireless, and mobile technologies.

Quarantine: Enforced isolation or restriction of communications imposed to prevent the introduction or spread of computer viruses.

RADIUS: Short for Remote Authentication Dial-In User Service. A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate remote users and authorize their access to the requested system or service.

Retention Schedule: The defined period of time for which electronic data must be retained and accessible in support of business and legal requirements.

Sanitization: The process for deleting sensitive data from a file, device, or system; or for modifying data so that it is useless if accessed in an attack.

SCADA: An acronym for Supervisory Control And Data Acquisition, a process control application that collects data from sensors and machines on a shop floor or in remote locations and sends them to a central computer for management and control.

Security: An attribute of information systems which includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services and the privacy of individuals.

Security Audit: A search through an information system designed to detect security problems and vulnerabilities and measure compliance to security policies and standards.

Secure Channel: Refers to information sent encrypted over the network.

SNMP: An abbreviation for Simple Network Management Protocol, an Internet standard that defines methods for remotely managing active network components such as servers, switches, hubs, routers, and bridges.

Source Code: The readable form of code that you create in a high-level programming language. Source code is converted to machine-language object code by a compiler or interpreter.

Split Knowledge: Separation of data into two or more parts. Each part is constantly kept under control of separate authorized individuals or teams so that no one individual or team will know the whole data.

Split Tunneling: Simultaneous access to a non-City network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the City network via a VPN connection.

SSH: Short for Secure Shell. A protocol for creating a secure connection between two systems using a client/server architecture. SSH provides mutual authentication, data encryption and data integrity.

SSID: Also know as a service set identifier. A unique identifier that stations must use to be able to communicate with a wireless access point.

Stateful Packet Inspection Firewall: A firewall that tracks the state of network connections traveling across it. This type of firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state are allowed through the firewall.

Strong Authentication: Strong authentication, also called two-factor authentication, is defined as providing two out of the following three proofs of identity: 1) something known, like a password, 2) something possessed, like an ATM card, and 3) something unique about a person, like a fingerprint.

System Operators: BTS and/or bureau technical support staff who implement, conduct routine day-to-day tasks, and maintain information systems, including authorization tables, security systems and back-up systems, in accordance with established City of Portland enterprise and business-specific policies, standards, procedures and guidelines.

Tamper: To interfere improperly or in violation of policy or rule such as to tamper with computing software or systems.

Token: A hardware device or software program that generates a one-time password to authenticate its owner or authorized user.

Trust Relationship: The relationship between two domains that enables a user or resource in one domain to access resources in another domain

Trojan Horse: Software that is written to allow access to a computer via some method not intended by the owner of the system. Typically embedded in some other form of software Trojan code attempts to camouflage its presence to avoid detection.

Untrusted Network: A network not controlled and configured by the Bureau of Technology Services.

USB Thumb Drive: A small, removable solid state data storage device which can be easily connected to and removed from a computer via its universal serial bus (USB) port.

Users: Any individual that has been granted privileges and access to computing, cummunications and network services, applications, resources, and information.

User Name: The name that identifies a user to a computer network; generally used in conjunction with a password to establish the user's right to access a host; also called account name or user ID.

Virtual Private Network (VPN): A way to provide remote access to an organization's network via a secure communications tunnel over the Internet

Virus: A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer. A true virus cannot spread to another computer without human assistance

Waiver: The voluntary and intentional relinquishment of a known right, claim or privilege.

Web Service: A Standardized way of integrating web-based applications which share business logic, data and processes through a programmatic interface across a network.

Wireless: Communications in which electromagnetic waves, rather than cables or wires, carry the signal over part or all of the communication path

Worm: A software programs capable of reproducing itself that can spread from one computer to the next over a network without human assistance

---

History
Ordinance No. 179999, passed by City Council March 15, 2006 and effective April 14, 2006. Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 5, 2009.