Document Type:	Regulation
Number:	4.30a
Effective:	05-01-06
Revised:	10-01-07
	06-16-09
	01-01-11
	06-09-14
	07-15-21
	07-12-22
Legal References:	

INFORMATION TECHNOLOGY ACCEPTABLE USE

I. INTRODUCTION

This regulation sets forth the City of Boise (the "city") acceptable use of its information assets and is applicable to employees, elected and appointed officials, volunteers, contractors, and interns (collectively, "Users") when using the city's information assets.

II. PURPOSE AND SCOPE

The purpose of this regulation is to outline the acceptable use of the city's information assets to protect the User and the city. Inappropriate use exposes the city to significant risks including virus attacks, compromised network systems and services, and legal issues.

A. This regulation applies to the use of all city information assets used to conduct city business or interact with internal networks and business systems, whether owned or leased by city, the User, or a third party. Information assets include but are not limited to the following:

   1. Software, including all programs and data stored and maintained on any media that are used on city equipment and/or all data owned by the city.
   2. Hardware, including electronic and computing devices, desktop and laptop computers, tablets, networks, Internet services, telephones, pagers, mobile devices, printers, fax machines, radios, other physical components, any device that uses city-provided services or capabilities, and all assets and resources owned or leased by the city whether or not they are accessed from city premises.

3. Services, including computer accounts for a User and the services provided by use of those accounts or use of the Internet, the city's wide area networks, local and long-distance telephone service, email, collaboration, and mobile telephone services, including additional capabilities such as text messaging. Services also include those not provided by the city but used to transact city business.

B. All Users are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with city policies, regulations, standards, and procedures, as well as all applicable laws and regulations.

III. GENERAL USE AND OWNERSHIP

city proprietary information stored on electronic and computing devices, whether the device is owned or leased by city, the employee or a third party, remains the sole property of the city.

A. All Users shall make every effort to ensure, through legal or technical means, that proprietary information is protected from theft, loss, or unauthorized disclosure.

B. All Users shall immediately report the theft, loss, or unauthorized disclosure of city proprietary information to their supervisor and IT.

C. Users may access, use, or share city proprietary information only to the extent authorized and necessary to fulfill assigned job duties.

D. For security and network maintenance purposes, authorized Users may monitor equipment, systems, and network traffic at any time, per IT Audit Policy.

E. The city reserves the right to audit networks and systems on a periodic basis to ensure compliance with this regulation.

F. Personal Use

1. Personal use of the city's information assets is not a part of the benefits package of any User. Although limited personal use of information assets may be permissible, in accordance with the specific provisions of this regulation and other city policies and regulations, such use does not give a User a right or entitlement to such access and use.

2. city information assets are provided by the city for business use. Limited personal use is allowed. Limited use is defined as occasional or incidental. Users are expected to exercise reasonable restraint regarding the frequency and duration of their personal use, and limit personal use to breaks, lunch periods, and off-duty time. Personal use shall not interfere with business needs, operations, or productivity.

3. The city will not provide technical support for personal devices or accounts except as specifically permitted in city policies and regulations.
4. The city will not provide in-person technical support for city-owned equipment at Users' residence or other personal remote work location.
5. Users shall exercise good judgment regarding the reasonableness of personal use. If there is any uncertainty, Users should consult their supervisor or manager.

IV. PERSONALLY OWNED MOBILE PHONES

The city allows the use of personally owned mobile phones for Users in positions that include a legitimate business need for a mobile phone. Users who use a personally owned device to access city systems or data outside of Web-based access shall install on the device and grant appropriate privileges to the city's Mobile Device Management solution.

Further guidance on mobile device usage and reimbursement may be found in the "*Mobile Device (Cellular Phone) Usage and Reimbursement*" regulation.

V. MONITORING

The city monitors the use of its information assets to provide protection and ensure that the assets are used effectively, appropriately, and legally.

A. The city may monitor information asset use in response to a particular problem, randomly, or in some cases, continuously on all activity related to city business or interests for a particular resource. The city reserves the right to inspect any files stored in private areas of its networks and systems to ensure compliance with the law, this regulation, and other city policies, regulations, and standards. The city may also choose or be required to publicize data obtained through monitoring.

B. The city monitors the use of some facilities using cameras, closed circuit television, identification badges, biometric identification devices, sign-in rosters, vehicle gates, access restrictions, security tools, and/or guards.

C. Personnel tasked with monitoring shall do so only when authorized by Human Resources or Legal and shall maintain confidentiality of all resulting information except as expressly directed. Information Technology shall establish a procedure for monitoring network activities and Security Operations shall establish a procedure for monitoring the security systems.

D. Interference with monitoring is prohibited. Interference includes but is not limited to encrypting information, notifying the person being monitored, or actively interfering with the monitoring process.

VI. PRIVACY

A. Users should not consider any electronic communication, media, or services to be either private or secure. Although email, computer and network accounts are protected by passwords, Users should understand that their account and records may not be private.

B. Users expressly waive any right of privacy in anything they create, store, send, or receive on a city device or through the city-provided Internet. This includes, but is not limited to, messages or data sent or received on a city-owned mobile device or on a personally owned mobile device while using city information assets through the city's Mobile Device Management solution.

C. Any communication or data transiting, stored on, or traveling to or from the city network and/or systems will be monitored and may be disclosed to outside agencies or used for any lawful government purpose.

D. The use of personally owned mobile devices to send and/or receive electronic communications via text message and/or personal email accounts for the transaction of city business creates a record that may be subject to disclosure pursuant to a public records request. Users who use personally owned mobile devices to transact city business may be required to provide all communications that relate to city business, including text messages, to the city upon request. The city strongly discourages the transaction of city business via text message on personally owned mobile devices and/or the transaction of city business via personal email accounts.

E. User accounts and data may be shared or accessed by the following positions:

   1. User's Supervisor.
   2. The User's Senior Manager, if applicable.
   3. Department Director.
   4. HR authorized personnel.
   5. Police Internal Affairs.

Users can share their data with other city Users with a business need to know.

VII. PASSWORDS

Passwords are the fundamental security mechanism employed to keep information secure and to associate activity with a User. Therefore, Users shall not:

A. Share, tell, or give hints about their passwords.

B. Keep a written unsecured record of their passwords.
C. Store passwords in a media cloud (Dropbox, Google Docs, etc.) other than city-approved secure repositories.
D. Mix city systems passwords with personal passwords in a password locker.
E. Store passwords on a device that others have access to; or
F. Email passwords via Gmail, Hotmail, etc.

All Users shall comply with the city's network password construction requirements as defined in the *Password Management Standard* found in *Exhibit 4.30aa*.

Users who suspect any of their passwords have been compromised shall change the affected password immediately.

If department management needs to access information in a User's account in accordance with this regulation, they are to contact the IT Customer Service Center for assistance.

VIII. INAPPROPRIATE USE

The city's information assets are provided to enhance business processes within the city. Use that is legal and business-related is appropriate. Users are prohibited from using the city's information assets to engage in, or attempt to engage in, activities including but not limited to the following:

A. Transmit, view, retrieve, copy, or store any communication that is:
    1. Discriminatory or harassing.
    2. Derogatory to any individual or group.
    3. Obscene or inappropriate for the workplace.
    4. Defamatory or threatening.
    5. Harmful to productivity; or
    6. Engaged in for any purpose that is illegal or contrary to city's policies, regulations, or procedures.
B. Sending uninvited and/or unwelcome electronic communication of a personal nature.
C. Downloading and distributing material protected under copyright laws without the proper consent of the owner, or otherwise violating copyright laws or other applicable laws.
D. Providing access to or copies of city information, data, hardware, software, or access to city services to third parties without adhering to approved procedures and authorization.

E. Accessing or using another User's account or failing to keep the User's own log-in or password confidential.

F. Sending any communication that attempts to hide the identity of the User or represents the User as someone else.

G. Downloading or transferring any files to any city systems, including entertainment software or games, that are not business related.

H. When using a personal email account at work and/or using city equipment, Users should never open any attachment to an email they receive. Users may be held accountable for damages sustained by viruses or other software that originated from personal email accounts.

I. Using the city's information assets for personal benefit or gain.

J. Using unauthorized technology resources on city networks including, but not limited to, personally owned equipment such as computers, printers, software, modems, and wired or wireless networking devices.

K. Sending business-sensitive information using Internet-based email accounts.

L. Using information assets in a manner that is likely to cause network congestion or significantly hamper the ability of other Users to access and use the city's information assets.

M. Distributing or storing chain letters, inappropriate jokes, solicitations or offers to buy or sell goods, or other non-business material of a trivial or frivolous nature.

N. Using the network to sign up with websites or organizations that offer rewards, monetary or otherwise, for surfing the internet.

O. Intentionally propagating a virus, worm, Trojan horse, or trap-door program code.

P. Blogging during work hours or while using city equipment.

IX. SOCIAL MEDIA

For information on the city's rules regarding the administration of social media, please refer to the *Social Media Administration Regulation 4.30m* and accompanying *Exhibit 4.30mm*.

For information on the city's rules regarding personal use of social media, please refer to the *Social Media Personal Use Regulation 4.30n*.

X. CITYWIDE MESSAGES

Users shall not send citywide messages unless they have been designated as a citywide email distributor by their Department Director and have the required system permissions. Each Department Director shall name one or more of these designated distributors as their department's "citywide email manager."

Users who are not designated as a citywide distributor and who believe they have a message of citywide interest shall bring the message to their department's citywide email manager for approval. If the citywide email manager determines the proposed message falls within the citywide email parameters, the citywide email manager will send out the proposed message. A list of current designated citywide email distributors and each department's citywide email manager can be obtained by contacting the IT Helpdesk.

The Citywide email parameters are as follows:

A. The proposed email message should be related to the business and mission of the city.

B. The message should be of significant and urgent interest to a large segment of city employees. In addition, events publicized over citywide email must be of a high-profile nature.

C. Messages should be short and concise. For topics that require more information, consider a summary email message that contains a link to more detailed information.

D. Emails of a personal nature, such as notices of items for sale, lost or found items and solicitation of goods or services are not allowed.

XI. ACCIDENTAL/UNINTENDED VIOLATIONS

The city follows best practice recommendations to block User access to inappropriate and/or sexually explicit Internet sites within its information assets.

A. Users who find themselves connected accidentally to a site that contains sexually explicit or other prohibited material shall disconnect from that site immediately, regardless of whether the site was somehow accessible to the employee.

B. Users who accidentally access a prohibited site shall report each incident to the User's supervisor and IT immediately. Repeated access to such sites by a User may be investigated to determine if such access is intentional.

XII. SOFTWARE COMPLIANCE

The city adheres to software licensing agreements. IT electronically monitors the software installed on all city computers and these scans are then compared to software licenses. IT is responsible for maintaining a list of approved software within the city. Employees shall not download or install any software that has not been approved by IT.

XIII. MANDATORY REPORTING OF VIOLATIONS

All suspected policy or regulation violations, system intrusions, and other conditions that might jeopardize the city's information assets shall be reported to IT immediately. Users shall report any weaknesses in city computer security and any incidents of possible misuse or violation.