CITY OF SPRINGFIELD

Information Technology (I.T.)

Information and Cyber Security

Administrative Regulation | Communication & Technology Standards | #14.07

Effective Date:	October 1, 2020
Revised Date:	January 12, 2026
Supersedes:	October 1, 2020

Note: Terms that are ***bolded and italicized*** the first time they appear in this regulation are defined below. After the first occurrence, defined terms appear in *italics only*.

Purpose

This administrative regulation explains how the City protects digital information and systems from cyber threats. It outlines employee responsibilities and City-wide IT security processes designed to reduce risks and ensure secure, reliable delivery of City services.

Scope

This regulation applies to all City of Springfield elected officials, employees, contractors, consultants, and any other individuals authorized to access information or systems owned, operated, or managed by the City.

The guidelines follow the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF): Identify, Protect, Detect, Respond, and Recover. Control measures are based on the Center for Internet Security (CIS) standards and other best recognized industry practices.

If an employee works with vendors, the employee must ensure contracts or service agreements include the applicable cybersecurity requirements outlined in this regulation.

Policy

Employees are expected to comply with the Oregon Identity Theft Protection Act (ORS 646A.600–628), including the requirement to implement a cybersecurity program (ORS 646A.622(d)).

Failure to comply with this regulation may increase risk to City operations and expose the City to legal action, penalties, and fines. Any ***data breach*** affecting 250 or more individuals may require reporting to the Oregon Department of Justice in accordance with applicable law and DOJ requirements.

Procedure

1. <u>Governance and Responsibilities</u>

a. The Information Technology Director (or designee) is responsible for overall administration of the City's cybersecurity program, including standards, tools, and oversight.

b. The Network Manager (or designee) is responsible for access control administration, monitoring, incident coordination, and approvals described in this regulation.

c. Department directors are responsible for ensuring staff comply with this regulation and for coordinating with IT regarding data ownership, business needs, and risk controls.

d. All users of City systems are responsible for protecting City information, complying with training requirements, and reporting suspected incidents promptly.

e. Vendors and service providers accessing City systems or data must comply with contractual cybersecurity requirements and City access controls.

2. <u>Asset Management</u>

a. The IT Department maintains an inventory of approved hardware and software on the City network. This inventory includes:

(1) The employee assigned to the asset.
(2) Purchase date.
(3) Serial number.
(4) Device type and description.
(5) Restricted software or devices

3. <u>Data Classification and Handling</u>

A. ***Personally Identifiable Information (PII) Inventory***

a. IT will initiate an annual update to compile and inventory all *PII* by type and location.

b. Department directors will coordinate with IT or Risk Management to determine if *PII* is essential.

(1) If *PII* is not essential, it will either not be collected, or (if previously collected) will be destroyed, subject to requirements of the Oregon Public Records Law and the City's Records Retention and Destruction Policy.

(2) All *PII* no longer needed shall be shredded by departments if in paper form or destroyed by IT if in electronic form, according to requirements of the Oregon Public Records Law and the City's Records Retention and Destruction administrative regulation.

B. **Oregon Identity Theft Protection Act Requirements**

a. Unless exempted by State or Federal law, the City will comply with the Oregon Identity Theft Protection Act by prohibiting anyone from:

(1) Printing a consumer's Social Security Number (SSN) on any mailed materials not requested by the consumer unless redacted;

(2) Printing a consumer's SSN on a card used by the consumer that is required to access products or services; and

(3) Publicly posting or displaying a consumer's SSN, such as on a website.

b. For purposes of applying these controls, “consumer” includes employees, applicants, and community members whose personal information the City maintains, where applicable.

C. **Data Classification**

a. Data residing on City systems must be continually evaluated by the IT Department and classified into the following categories:

(1) _Personal Use_: Includes individual users’ personal data, emails, and documents stored on City systems. Personal data stored on City systems is not exempt from monitoring, public records obligations, or security controls.

(2) _Public/Informational_: Includes published marketing material, commonly known information, and data intended for public release. Public information must still be protected against unauthorized modification.

(3) _Operational_: Includes data for basic organizational operations, communications with vendors, employees, etc. that are not confidential. The majority of data will fall into this category.

(4) _Restricted_: Information requiring heightened safeguards due to legal, privacy, safety, or security risk, including *PII*/*PHI*, security configurations, ***privileged*** credentials, and other sensitive regulated data.

(5) _Confidential_: Any information deemed confidential by law, contract, or City designation. ***Confidential data*** may include:

(i) Employee or customer SSN or personally identifiable information (*PII*);
(ii) Personnel files;
(iii) Medical and healthcare information;
(iv) ***Protected Health Information (PHI***);
(v) Network diagrams and security configurations;
(vi) Communications regarding legal matters;
(vii) Passwords/passphrases;
(viii) Bank account information and routing numbers;
(ix) Payroll information;
(x) Credit card information; and
(xi) Any *confidential data* held for a third party (be sure to adhere to any *confidential data* agreement covering such information).

4. Identity Management, Authentication and Access Control

a. The Network Manager or designee is responsible for ensuring that access to the City's systems and data is appropriately controlled.

b. Wherever possible, systems housing data (including laptops, desktops, tablets, and cell phones) must be protected with a password or other form of authentication.

c. Except for the instances noted in this policy, users with access to City systems and data are not to share passwords with anyone.

d. Where applicable, the City has established the following password configuration requirements for all systems and applications:

(1) Minimum password length: 8 characters.
(2) Password complexity: requires alphanumeric and special characters.
(3) Password reuse: prohibited for at least four (4) previous iterations.
(4) Password change frequency: required at least once every 90 days.
(5) Invalid login attempts: Limited to three (3) consecutive failures.
(6) Session timeout: automatic logout after thirty (30) minutes of inactivity.

e. Other potential safeguards include:

(1) Not allowing *PII* on mobile storage media;
(2) Locking file cabinets;
(3) Not allowing *PII* to be left on desks;
(4) Encrypting sensitive files on computers;
(5) Requiring password protection; and
(6) Implementing the record retention plan and destroying records no longer required

f. Where possible, ***multi-factor*** authentication will be used when users access the City's systems.

g. Users are granted access only to the system data and functionality necessary for their job responsibilities.

h. *Privileged* and administrative access is limited to authorized users who require escalated access for their job responsibilities and where possible will have two accounts:

(1) one for administrator functions; and
(2) a standard account for day-to-day activities.

i. All user access requests must be approved by the Network Manager or their designee.

j. It is the responsibility of the Network Manager or their designee to ensure that all employees and contractors who separate from the organization have all system access removed within twenty-four (24) hours of notice.

k. On an annual basis, a review of user access will be conducted by the IT department under the direction of the Network Manager or designee to confirm compliance with the access control policies outlined above.

5. <u>Awareness and Training</u>

a. The City will strive to implement the following training:

(1) *New Hire Training*: All new hires are required to complete security awareness training before receiving full login credentials. Upon completion of training, participants will review and sign the Acceptable Use of City Network Services & Computing Devices Administrative Regulation form.

(2) *Annual Training*: Formal security awareness refresher training is conducted on an annual basis. All employees are required to participate in and complete this training.

b. The City will conduct annual email phishing exercises.

(1) The purpose of these tests is to help educate users on common phishing scenarios.

(2) Exercises will assess awareness of phishing, safe handling of emails containing links/attachments, and ability to recognize questionable or fraudulent messages.

6. Data Storage Transmission, Encryption, and Destruction

A. Data Storage Types

a. The following guidelines apply to storage of organizational data:

(1) *Operational*: Operational data should be stored on a server that receives frequent backups. System- or disk-level redundancy is encouraged.

(2) *Confidential*: Confidential information must not be left visible on screens or in common areas unless currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with access secured.

B. Data Transmission

a. The following guidelines apply to the transmission of the different types of organizational data. Wherever possible, *confidential data* must not be:

(1) Transmitted outside the organization's network without the use of strong encryption.
(2) Left on voicemail systems, either inside or outside the organization's network.

b. For City purposes, “organization” means the City of Springfield.

C. Encryption

a. Stored data on City-owned or City-provided systems, devices, media, or backups will be encrypted when possible. Examples include:

(1) Whole disk encryption;
(2) Encryption of partitions/files;
(3) Encryption of disk drives;
(4) Encryption of personal storage media/USB drives;
(5) Encryption of backups; and
(6) Encryption of data generated by applications.

b. Data transmitted across City network or sent to/from a City-owned or City-provided system shall be encrypted when possible, including:

(1) VPN tunnels;
(2) Remote access sessions;
(3) Web applications;
(4) Email and email attachments;
(5) Remote desktop access; and
(6) Communications with applications/databases.

D. **Data Destruction**

a. City users will follow the City's Records Retention and Destruction administrative regulation before destroying data.

b. *Confidential data* must be destroyed in a manner that makes recovery of the information impossible.

c. Guidelines:

(1) *Paper/documents*: Cross-cut shredding is required.

(2) *Storage media* (CD's, DVD's): Physical destruction is required.

(3) *Hard drives/systems/mobile storage media*:

(i) At a minimum, data wiping must be used.

(ii) Simply reformatting a drive does not make the data unrecoverable.

(iii) If wiping is used, the organization must use the most secure commercially available methods for data wiping.

(iv) Alternatively, the organization has the option of physically destroying the storage media.

7. Secure Development and Change Management

A. **Secure Software Development**

a. Where applicable, all software development activities performed by the City or by vendors on behalf of the City shall employ secure coding practices including those outlined below.

b. Where feasible, the City will use development, quality assurance and production environments when developing software systems.

c. Developers will develop and promote objects into QA and production.

d. QA will be used for assurance testing by the end user and the developer.

e. Production us used solely for production data and applications. Compiling objects and the source code is not allowed in the production environment.

f. All production changes must be approved before being promoted to production.

g. All production changes must have a corresponding help desk change request number.

h. All production changes should be developed in the development/test environment.

i. Emergency changes should be documented and approved per IT procedures.

8. Backup and Contingency Planning

a. The City's contingency capability is based upon both cloud and local backups of critical business data.

b. Full data backups will be performed at least weekly by IT.

c. IT will confirm successful backups monthly.

d. Testing of cloud backups and full restoration testing of critical system backups should be performed annually.

e. During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the IT Director or designee in connection with Risk Management, City Attorney's Office and City Manager's Office as required.

f. Contingency scenarios and responses:

(1) In the event that one or more of the City's systems or applications are deemed corrupted or inaccessible, the Network Manager or designee will work with the respective vendor(s) to restore data from the most recent backup and, if necessary, acquire replacement hardware.

(2) In the event that the location housing the City's systems are no longer accessible, the Network Manager or their designee will work with the respective vendor(s) to acquire any necessary replacement hardware and software, implement these at one of the organizations other sites, and restore data from the most recent backup.

9. Infrastructure Security

A. Network Infrastructure

a. The City will protect the organization's electronic communications network from the Internet by utilizing a firewall.

b. Network devices should meet configuration standards:

(1) Vendor-recommended and industry standard configurations will be used.

(2) Changes to firewall and router configuration must be approved by the Network Manager or designee.

(3) Router and firewall passwords must be secured and difficult to guess.

(4) Default inbound firewall policy should block all connections unless specifically permitted.

(5) Inbound ICMP traffic should not be passed in from the Internet, or untrusted networks.

(6) Web services running on routers must be disabled.

(7) Simple Network Management Protocol (SNMP) Community Strings must be changed from the default settings.

B. **Network Servers**

a. The City will follow the following guidelines when possible:

(1) Unnecessary files, services, and ports should be removed or blocked.
(2) Network servers must be protected by a firewall or access control list.
(3) A standard server installation process should be developed when feasible.
(4) Server clocks should be synchronized using NTP or another standards.

C. **Network Segmentation:**

a. Network segmentation limits access to data based on sensitivity.

(1) The City maintains two wireless networks.
(2) The guest wireless will grant the user internet access only.
(3) Access to the secure wireless network is limited to City's personnel.

b. Under the direction of the Network Manager or their designee, Lane County IT manages the network user accounts, monitors firewall logs, and operating system event logs.

c. The Network Manager or their designee authorizes vendor access to the system components as required for maintenance.

10. <u>Protective Technology</u>

A. **Email Filtering**

a. The City will filter email at the Internet gateway and/or the mail server to reduce spam, viruses, or other messages that may be deemed either contrary to this policy or a potential risk to the organization's IT security.

b. McAfee Quarantine Manager has been implemented to identify and quarantine emails that are deemed suspicious.

B. **Vulnerability Assessments and Testing**

a. The City will perform both internal and external network vulnerability assessments.

(1) These evaluations will be conducted under the direction of the Network Manager or their designee to identify weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization's data and systems.

b. Penetration testing may be conducted only with approval and must not disrupt City systems or operations.

11. Logging and Event Management

a. Logging activities under the direction of the Network Manager or designee include:

(1) *Domain Controllers*: Active Directory event logs will be configured to log the following security events: account creation, escalation of privileges, and login failures.

(2) Application Servers: Logs from application servers (e.g., web, email, database servers) will be configured to log the following events: errors, faults, and login failures.

(3) *Network Devices*: Logs from network devices (e.g., firewalls, network switches, routers) will be configured to log the following events: errors, faults, and login failures.

b. Passwords should not be contained in logs.

c. The City will strive to implement tools to review the logs above.

12. Continuous Monitoring and Patch Management

A. Anti-Malware Tools

a. All City servers and workstations will utilize antivirus and malware software to protect systems from malware and viruses.

b. Real-time scanning will be enabled on all systems and weekly malware scans will be performed.

c. The Network Manager or their designee will review the dashboard monthly to confirm the status of virus definition updates and scans.

d. The City will work toward using a tool to protect mobile devices from malware and viruses.

B. Patch Management

a. All software updates and patches will be distributed to all City systems as follows:

(1) Workstations configured to install software updates automatically monthly.
(2) Server updates manually installed at least monthly.
(3) Exceptions must be documented.

13. Incident Response and Notification

A. Response Planning

a. IT is responsible for annual security awareness training that includes incident types, actions to take, and reporting channels.

b. The Network Manager is responsible for coordinating activities during significant incidents, including notification and escalation and deciding if/when outside agencies, must be contacted.

B. **Electronic Incident:**

a. When an electronic incident is suspected:

(1) Remove the compromised device from the network by unplugging or disabling the connection.

(2) Do not power down the machine.

(3) Report the incident to the Network Manager or their designee and to the Risk Manager.

(4) The Network Manager or their designee, will notify the third-party service provider and/or forensic specialist as needed.

b. Remaining steps with third-party assistance as appropriate:

(1) Disable the compromised account(s).
(2) Backup or image the affected system.
(3) Determine what happened and the scope.
(4) Identify entry method and disable it.
(5) Rebuild systems, including full OS reinstall when required.
(6) Restore data from last known good backup and return to service.
(7) Implement controls to prevent recurrence.
(8) Conduct post-incident evaluation.

C. **Physical Incidents**

a. Physical incident includes loss or theft of a laptop, mobile device, smartphone, portable storage device, or other devices that may contain City information.

b. Report suspected physical incident immediately to the Network Manager or designee.

c. Suspected theft should also be reported to law enforcement.

D. **Notification:**

a. If an incident is suspected to have resulted in loss of third-party/customer data, the Network Manager and Risk Manager will notify:

(1) Insurance
(2) City Attorney
(3) Oregon Department of Justice, using the breach notification forms if the breach involves more than 250 records.

14. Recovery and Post-Incident Review

a. The Network Manager or designee manages recovery activities during an incident, including recovery steps.

b. The Network Manager or designee identifies, evaluates, and incorporates lessons learned into future activities and policies.

c. Restoration activities are coordinated with internal and external parties, including vendors and affected system owners.

d. External communications must be handled only by designated individuals under the direction of the Network Manager or designee.

e. Recovery activities will also be communicated to internal stakeholders and the Executive Team.

f. Incident response and recovery actions will be documented in accordance with record retention requirements.

Definitions

Term:	Definition
Data Breach:	Unauthorized acquisition of unencrypted personal information, or other breach definition as established by applicable law.
Confidential Data:	Information designated confidential by law, contract, or City classification, including sensitive personnel, legal, financial, and security information.
Cybersecurity Incident:	An event that results in, or could reasonably result in, unauthorized access to, disclosure of, modification of, or disruption to City systems or data.
Multi-Factor Authentication (MFA):	An authentication method requiring two or more verification factors to gain access to a system.
Personally Identifiable Information (PII):	Is personal information as defined in the Oregon Consumer Information Protection Act at ORS 646A.602(12). PII includes a first name or initial with last name together with any of the following: Social Security number; driver's license; state ID; passport; financial account or payment card numbers; biometric data; and health insurance or medical history information. PII also includes usernames or other identifiers used to permit access to a consumer's account together with any other method necessary to authenticate the username or identifier. When data is not encrypted and theft would enable identity theft, any of the foregoing information may be considered PII even in absence of a username or the combination of first and last name. PII does not include information in federal, state, or local government records lawfully made available to the public.
Privileged Account:	An account with administrative or elevated permissions capable of changing system configurations or accessing ***restricted data***.

Protected Health Information (PHI): Defined in HIPAA regulations at 45 CFR 160.103. *PHI* includes individually identifiable health information held or transmitted by a covered entity or business associate and related to an individual’s health condition, health care, or payment for health care.

Restricted Data: Information requiring heightened safeguards due to privacy, safety, security, or regulatory requirements, including PII, *PHI*, privileged credentials, and security configurations.

Related Resources

Administrative Regulations:

- Acceptable Use of Network and Computing Devices
- Records Retention and Destruction

Online Resources:

- US Department of Justice Breach notification website