Document Type:	Regulation
Number:	4.30p
Effective:	12-1-23
Revised:	

INFORMATION SECURITY REGULATION

1.0 Purpose and Benefits

This regulation defines the mandatory minimum information security requirements for the City of Boise (the city) as defined in Section 3.0, “Scope”. Any department may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this regulation.

This regulation acts as an umbrella document to all other IT security policies and associated standards. This regulation defines the city’s responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today’s highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This regulation benefits departments by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity, and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security regulation procedures, and practices, and know how to protect information. It complements the city’s Records Management Policy and Records Retention Schedule by specifying how city information, and by extension city records, should be protected, with particular focus on the information systems that maintain city information in electronic form.

2.0 Authority

The city's Information Security Regulation directs the Information Technology Department to establish policies, regulations, and procedures to express the city's philosophy regarding information security requirements and standards, and to set forth general information security principles with which employees, volunteers, contractors, and interns, collectively referred to as "Users," shall comply when using city information systems.

3.0 Scope

This regulation encompasses all systems, automated and manual, for which the City of Boise has administrative responsibility, including systems managed or hosted by third parties on behalf of the city. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

This regulation outlines essential requirements for safeguarding city information from unauthorized access, disclosure, alteration, or destruction. Other city policies, such as records management and continuity of operations (COOP), complement this regulation by specifying how city information is to be used and how the enabling information systems should be operated.

4.0 Information Statement

4.1 Organizational Security

a. Information security requires both an information risk management function and an information technology security function. These functions should be performed by a senior executive (department Director or Chief Administrative Officer) or a group that includes members of the city's Executive Management Team.
    1. The Director, Information Technology shall designate an individual or group to be responsible for the risk management function assuring that:
        i. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and

        ii. the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.

    2. The Director of the city's Information Technology Department shall designate an individual to serve as Chief Information Security Officer (CISO). This role will be responsible for developing and implementing a city information security program that will ensure compliance with the provisions of this Regulation.

3. Each city department shall designate an individual or group to be responsible for the department's technical information security function. For purposes of clarity and readability, this regulation will refer to these individuals or groups so designated as the Information Security Officer (ISO)/designated security representative. This function will be responsible for evaluating and advising on Department information security risks and will serve as single points of contact for Information Security issues.

b. Information security risk decisions must be made through consultation with both function areas described in **a.** above.

4.2 Functional Responsibilities

4.2.1 The City's Executive Management Team (EMT) is responsible for:

1. evaluating and accepting risk on behalf of the city;
2. identifying information security responsibilities and goals and integrating them into relevant processes;
3. supporting the consistent implementation of information security policies and standards;
4. supporting security through clear direction and demonstrated commitment of appropriate resources;
5. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO/designated security representative;
6. implementing the process for determining information sensitivity classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;
7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;
8. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
9. participating in the response to security incidents;
10. complying with notification requirements in the event of a breach of private information;
11. adhering to specific legal and regulatory requirements related to information security;

12. communicating legal and regulatory requirements to the ISO/designated security representative; and

13. communicating requirements of this regulation and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

4.2.2 IT management is responsible for:

1. supporting security by providing clear direction and consideration of security controls in the city's data processing infrastructure and computing network(s);

2. providing resources needed to maintain a level of information security control consistent with this regulation;

3. identifying and implementing all processes, policies, regulations, and controls relative to security requirements defined by the business, this regulation, and city code and Idaho State code.;

4. implementing the proper controls to assure appropriate information protection based on classification designations;

5. providing training to each Department's Information Security Officer or Group on security concerns and security compliance requirements and providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);

6. supporting and consulting with each Department's Information Security Officer or Group to identify security exposures, assess security compliance, and implement security controls.

7. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and

8. implementing business continuity and disaster recovery plans.

4.2.3 The CISO is responsible for:

1. providing in-house advisory security expertise as needed;

2. developing and executing the security program and strategy, including measures of effectiveness;

3. establishing and maintaining enterprise information security policies, regulations, and standards;

4. ensuring alignment with records management policies and standards;

5. assessing compliance with security policies, regulations, and standards;

6. advising on secure system engineering, and on security issues related to procurement of products and services;
7. providing incident response coordination and expertise;
8. monitoring systems and networks for anomalies;
9. monitoring external sources for indications of data breaches, defacements, etc.
10. maintaining ongoing contact with security groups/associations and relevant authorities;
11. providing timely notification of current threats and vulnerabilities; and
12. providing awareness materials and training resources, including focused training for department ISOs;
13. evaluating and understanding information security risks and how to appropriately manage those risks; and
14. representing and assuring security architecture considerations are addressed.

4.2.4 The Department ISO/designated security coordinators are responsible for:

1. maintaining familiarity with Department business functions and requirements;
2. assisting the CISO in promoting information security awareness;
3. maintaining an adequate level of proficiency in information security issues as warranted by business needs;
4. in collaboration with the CISO, disseminating threat information to appropriate parties when warranted;
5. participating in the response to potential or actual security incidents as necessary;
6. coordinating department participation in the development of Department standards and procedures that considers the city's needs; and
7. if appropriate to role and/or department, partnering with the CISO to assess Department compliance with information security policies and legal and regulatory information security requirements.

4.2.5 The workforce is responsible for:

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
2. protecting information and resources from unauthorized use or disclosure;

3. protecting personal, private, sensitive information from unauthorized use or disclosure;

4. abiding by the City's *Acceptable Use of Information Technology Resources Regulation; and*

5. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.

4.3 Separation of Duties

a. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate. "Separation of Duties" refers to the principle that no user should be given enough privileges to misuse a system on their own; for example, the person authorizing a paycheck should not also be the one who can prepare it.

b. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.

c. The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

4.4 Information Risk Management

a. Any system or process that supports business functions must be appropriately managed for information risk and undergo IT-led information risk assessments, at a minimum annually, as part of a secure system development life cycle.

b. Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.

c. Departments are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.

d. Risk assessment results, and the decisions made based on these results, must be documented.

4.5 Information Classification and Handling

a. All information which is created, acquired or used in support of business activities must only be used for its intended business purpose. Any such information is considered to be an "information asset".

b. All information assets must have an information owner established within the lines of business. An "information owner" is an IT and/or business data expert that defines

rules for usage, approves access, and approves data quality corrections and quality reporting metrics.

c. Information must be properly managed from its creation, through authorized use, to proper disposal in accordance with Idaho code and City of Boise Code and records management policies.

d. All information must be classified for its data sensitivity level on an ongoing basis based on its confidentiality, integrity, and availability characteristics.

e. An information asset must be classified based on the highest data sensitivity level necessitated by the nature of the individual data elements contained within the information asset.

f. If the city is unable to determine the confidentiality classification of information, or the information is personal identifying information (PII), the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.

g. Merging of information which creates a new information asset, or situations that create the potential for merging (e.g., backup tape with multiple files), must be evaluated to determine if a new classification of the merged data is warranted.

h. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.

i. Each classification shall have an approved set of baseline controls designed to protect these classifications and these controls must be followed.

j. The CISO shall communicate the requirements for secure handling of information to it's the city's workforce.

k. The IT Department shall maintain a written or electronic inventory of all information assets.

l. Content to be made available to the general public shall be reviewed prior to publication to ensure sensitive data will not be disclosed. The review process shall also include the review and approval of updates to publicly available content to consider the type and classification of information posted.

m. Personally Identifiable Information (PII) must not be made available without appropriate safeguards approved by the CISO.

n. For non-public information to be released outside the city or shared between other entities, a process must be established that, at a minimum:
    1. evaluates and documents the sensitivity of the information to be released or shared;

    2. identifies the responsibilities of each party for protecting the information;

3. defines the minimum controls required to transmit and use the information;

4. ensures the measures that each party has in place to protect the information are sufficient;

5. defines a method for compliance measurement;

6. provides a signoff procedure for each party to accept responsibilities; and

7. establishes a schedule and procedure for reviewing the controls.

4.6 IT Asset Management

a. Each IT hardware and software asset must be assigned to a designated Department or individual.

b. The IT Department shall maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory shall be automated where technically feasible.

c. The City shall design and implement controls to prevent users from installing unauthorized software on city hardware assets.

d. Audit processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

4.7 Personnel Security

a. New workforce members (city officials, employees, volunteers, contractors, and interns) shall receive general security awareness training within 30 days of hire.

    1. City officials, employees, and interns shall receive general security awareness training within 30 days of hire. All security training must be reinforced at least annually, and completion shall be tracked.

    2. Contractors and volunteers requiring access to city information systems shall be provided a copy of this regulation and be required to acknowledge reading and understanding its contents before beginning service with the city.

    3. For all workforce members, additional training on specific security procedures, if required, must be completed before access is provided to specific sensitive information not covered in the general security training.

b. The city shall require its workforce to abide by the Acceptable Use of Information Technology Resources Regulation, and an auditable process must be in place for users to acknowledge that they agree to abide by the regulation’s requirements.

c. All job positions must be evaluated by the city to determine whether they require access to sensitive information and/or sensitive information technology assets.

d. For those positions requiring access to sensitive information and sensitive information technology assets, Departments must conduct workforce suitability determinations when creating/updating a job description, unless prohibited from doing so by law, regulation, or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the Department to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the city.

e. A process must be established within the city to repeat or review suitability determinations upon change of job duties or position.

f. Departments are responsible for ensuring all issued property is returned prior to an employee's separation, and accounts are disabled, and access is removed immediately upon separation.

4.8 Cybersecurity Incident Management

a. The city shall have an incident response plan, with consistent standards, to effectively respond to security incidents.

b. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that information security concerns are not being appropriately addressed, they may confidentially contact the IT Department and/or CISO directly or escalate through their department management.

c. The Information Security team must be notified of any information security incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

4.9 Physical and Environmental Security

a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and physical access controls.

b. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. Any such measures must be implemented to mitigate the risks.

c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls shall be implemented as necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.

d. All information technology equipment and information storage devices must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.

e. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times by a city employee. Contractors may not escort other contractors. Maintenance personnel who have passed a full background check and have completed Criminal Justice Information Services (CJIS) training do not require an escort.

4.10 Account Management and Access Control

a. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the Department to which the individual is assigned and Information Technology (IT).

b. Access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs. Any exceptions must be explicitly approved by the CISO.

c. Associated with each user-ID is an authentication token (e.g., password, token, biometric) which must be used to authenticate the identity of the person or system requesting access. Automated techniques and controls must be implemented to lock or end a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, wallpaper, clock) during the session lock.

d. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.

e. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

f. Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the CISO and/or ISO/designated security representative.

g. Information owners are accountable for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).

h. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with City missions and business functions (i.e., least privilege).

i. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

j. Use of a privileged account on a city system must also require a second authentication factor other than a password.

k. Logon banners shall be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with regulation, and that user activities may be monitored, and the user should have no expectation of privacy.

l. Requests for remote access connections must be submitted in advance for City approval. An assessment shall be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.

m. All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.

n. Working from a remote location must be authorized by management, and practices which assure the appropriate protection of data in remote environments must be shared with, and acknowledged by, the requesting individual prior to the individual being granted remote access.

4.11 Systems Security

a. Systems include but are not limited to servers, platforms, networks, communications, databases, peripheral devices, and software applications.

    1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of the city. The IT Department will maintain list of assigned individuals or groups.
    2. Security must be considered at system inception and documented as part of the decision to create or modify a system.
    3. All systems must be developed, maintained, and decommissioned in accordance with a secure system development lifecycle (SSDLC).
    4. Each system must implement a set of controls commensurate with the classification of any data that is stored on or passes through the system.
    5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.

6. Environments and test plans must be established to validate each system works as intended, and required security controls function as designed, prior to deployment in production.
7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
8. Formal change control procedures for all systems must be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

    a. <u>Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):</u>
        1. All software written for or deployed on systems must incorporate secure coding practices to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
        2. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.
        3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:
            i. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
            ii. sensitive data is masked or overwritten with fictional information.
        4. Where technically feasible, development software and tools must not be maintained on production systems.
        5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
        6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
        7. Privileged access to production systems by development staff must be restricted and audited.
        8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

    b. <u>Network Systems:</u>

1. Connections between systems must be authorized by the executive management of all relevant Departments and protected by the implementation of appropriate controls.
2. All connections and their configurations must be documented, and the documentation must be reviewed by the information owner(s) and the ISO/designated security representative annually, at a minimum, to assure:
    i. the business case for the connection is still valid and the connection is still required; and
    ii. the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
    i. Internet accessible systems and internal systems;
    ii. systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and
    iii. user and server segments.
4. Network management should be performed from a secure, dedicated network.
5. Authentication is required for all users connecting to internal systems.
6. Network authentication is required for all devices connecting to internal networks.
7. Only authorized individuals or Departments may capture or monitor network traffic.
8. A risk assessment must be performed in consultation with the ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

4.12 Collaborative Computing Devices

a. “Collaborative Computing Devices” refers to equipment designed to facilitate and support collaboration among users, primarily in a conference room setting. Collaborative computing devices include interactive whiteboards, video conferencing systems, and virtual collaboration platforms that allow real-time collaboration on documents or projects. Collaborative computing devices must:
    1. prohibit remote activation; and
    2. provide users physically present at the devices with an explicit indication of use.
b. The IT Department must provide simple methods to physically disconnect collaborative computing devices.

4.13 IoT Devices

a. An IoT (Internet of Things) device is a device that can be connected to the internet (or to a city network) and can communicate with other devices or systems, often through wireless or wired networks. These devices are designed to collect and transmit data and can range from simple sensors to complex machines or appliances. Examples of IoT devices include smart thermostats, security cameras, fitness trackers, and industrial sensors.

b. All IoT devices must be secured with strong, unique passwords, and should be configured to use encryption where possible. Devices must be regularly updated with the latest firmware and security patches to mitigate against known vulnerabilities.

c. Devices must also be properly segmented within the network to limit access and contain potential security incidents. Access controls must be implemented to restrict access to IoT devices and data to authorized personnel only.

4.14 Vulnerability Management

a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

b. All systems are subject to periodic penetration testing.

c. Penetration tests are required periodically for all critical environments/systems.

d. Where the City has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing should be coordinated.

e. Scanning/testing and mitigation must be included in third party agreements.

f. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for evaluation of risk.

g. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

h. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

i. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

4.15 Operations Security

a. All systems and the physical facilities in which they are stored must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.

b. System configurations must follow approved configuration hardening standards.

c. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

d. Where the city provides a server, application or network service to another external entity, operational and management responsibilities must be coordinated by all impacted entities.

e. Host based firewalls must be installed and enabled on all mobile workstations to protect from threats and to restrict access to only that which is needed.

f. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.

g. Controls must be implemented to disable automatic execution of content from removable media.

h. Controls must be implemented to limit storage of information to authorized locations.

i. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.

j. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

k. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process should be automated, where technically possible.

l. Systems which can no longer be supported or patched to current versions must be removed as soon as feasible. Mitigating controls must be put in place until the system is removed. Exception requests shall be submitted to the CISO for review and approval.

m. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this regulation, and to record events to provide evidence and to reconstruct lost or damaged data.

n. Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with record retention schedules and requirements.

o. Monitoring systems (e.g., intrusion detection/prevention systems) must be deployed at strategic locations to monitor inbound, outbound, and internal network traffic.

p. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

q. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested annually or as specified in the city's Continuity of Operations (COOP) plan. Contingency plans shall address, at minimum, the following:
    1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

    2. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical systems.

r. Backup copies of city information, software, and system images must be taken regularly in accordance with the city defined requirements.

s. Backups and restoration must be tested regularly to ensure restoration integrity and completeness. Separation of duties must be applied to these functions.

t. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

u. Systems being retired or decommissioned must be properly sanitized prior to being surplused or disposed of to ensure no city data remains in a retrievable form. Records management requirements must be considered in this process.

5.0 Compliance

This regulation shall take effect upon publication. Compliance is expected with all city policies, regulations, and standards. Policies, regulations, and standards may be amended at any time; compliance with amended policies, regulations, and standards is expected.

If compliance with this Regulation is not feasible or technically possible, or if deviation from this Regulation is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition
Information Security	Information security refers to the practice of protecting information by mitigating information risks. It involves the implementation of measures, processes, and policies to safeguard data and information systems from unauthorized access, disclosure, alteration, or destruction, ensuring the confidentiality, integrity, and availability of critical information assets. Information security aims to prevent data breaches, cyberattacks, and other threats that could compromise the security and privacy of sensitive information.
Information System	An information system is a structured and organized collection of hardware, software, data, processes, and people that work together to capture, process, store, transmit, and manage data and information within the city.
Data Asset	A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. Note that a database is a data asset that is comprised of data records, so a data asset should be considered to be a collection of records.
Baseline Controls	Baseline controls comprise the set of fundamental security measures and practices that establish a minimum standard for protecting city information assets from common threats and vulnerabilities.
ISO	Information Security Officer. An individual or group responsible for the technical information security function and for evaluating and advising on information security risks.
CISO	Chief Information Security Officer. The individual responsible for developing and implementing the City's information security program.
CJIS	Criminal Justice Information Services (CJIS) is a division of the FBI responsible for establishing nationwide requirements, guidelines, and standards for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI).
PII	Personally Identifiable Information (PII) is information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers (e.g., passport information) that alone can identify a person uniquely, or other identifiers that can be

Term	Definition
	combined (e.g., name plus date of birth) to identify the person uniquely. The State Code definition of PII is as follows: “"Personal information" means an Idaho resident’s first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) Social security number; (b) Driver’s license number or Idaho identification card number; or (c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial account. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.”
RTO	Recovery Time Objective. Specifies the maximum amount of acceptable system downtime in case of an event that causes a system outage.
RPO	Recovery Point Objective. Specifies the maximum amount of acceptable transactional data loss in case of an event that causes a system outage.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the IT Cybersecurity Team.

8.0 Revision History

This regulation shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
3/17/2023	Initial Draft	Cybersecurity Team
7/7/2023	Incorporate CIO feedback	Cybersecurity Team
10/2/2023	Incorporate Key Stakeholder Feedback	Cybersecurity Team
10/10/2023	Incorporate final review feedback	Cybersecurity Team
11/1/2023	Final version for EMT Review	ISD

9.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations