DATA PRIVACY AND SECURITY REQUIREMENTS FOR IT SYSTEMS

Spokane Workforce Council Administrative Policies and Procedures **Effective Date:** March 2021

1. Background

Federal and Washington state law, Office of Management and Budget (OMB) guidance, and Department of Labor (DOL) and Employment and Training Administration (ETA) policies require that privacy and security of personally identifiable information (PII) and other sensitive or confidential information be protected. As stewards of Federal funds handling PII and other potentially sensitive and confidential information, the Spokane Workforce Council (SWC) has a responsibility to secure the use, storage, and transmission of data. This policy describes the requirements for protecting the confidentiality, integrity, and availability of data; assessing and mitigating security risks to data; and keeping security practices current and relevant.

2. Definitions

- **Data classification:** a category of information based on the sensitivity and confidentiality requirements of the data, as specified in Office of the Chief Information Officer (OCIO) Policy 141.10, other Washington state laws, and Training and Employment Guidance Letter (TEGL) 39-11, which includes the following categories:
    - **Category 1 – Public Information:** public information is information that can be or currently is released to the public and does not require protection from unauthorized disclosure.
    - **Category 2 – Sensitive Information:** any information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or conduct of the SWC, its subrecipients, or the privacy to which individuals are entitled under the Privacy act. Sensitive information is not specifically protected from release or disclosure by law. Sensitive information is generally not released to the public unless specifically requested.
    - **Category 3 – Confidential Information:** confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:
        - **Protected PII:** information that if disclosed could result in harm to the individual whose name is linked to that information or that can be used to distinguish or trace an individual's identity on its own. Examples of protected PII include, but are not limited to:
            - Full social security number (TEGL 39-11);
            - Account number, credit or debit card number, or bank account number associated with an individual's financial account (TEGL 39-11);
            - Username or email address in combination with a password or security questions and answers that would permit access to an online account (RCW 42.56.590(10)(a)(ii));
            - Any information, that when combined with an individual's first name (or first initial) and last name, is linkable to a specific individual, including but not limited to (TEGL 39-11 & RCW 42.56.590(10)(a)(i)):
                - Last four digits of a social security number;
                - Driver's license number or Washington identification card number;
                - Student, military, or passport identification number;
                - Home telephone number;
                - Age;
                - Full date of birth;
                - Spouse's name;
                - Marital status;
                - Educational history;

- Biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;
- Financial information or any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account;
- Health insurance policy or identification number;
- Device or lock password or passcode;
- Private key that is unique to an individual and that is used to authenticate or sign an electronic record;

- Any information, that when combined with two or more elements of other personal information, is linkable to a specific individual, including but not limited to (TEGL 39-11):
  - First name (or first initial) and last name;
  - E-mail address;
  - Business address or business telephone number;
  - General education credentials;
  - Gender;
  - Race or ethnicity;

Note: Personally identifiable information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records (RCW 19.255.005(3) & RCW 42.46.590(10)(a)(i)).

- **Lists of individuals for commercial purposes:** though first name (or first initial) and last name are not confidential by themselves, lists of individuals by name must be protected from release or disclosure for commercial purposes (RCW 42.56.070 (8)).
- **Network infrastructure and security information:** information regarding the infrastructure and security of computer and telecommunications networks owned or utilized by the SWC is considered confidential and consists of: security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, security test results to the extent that they identify specific system vulnerabilities, and other such information that the release of which may increase risk to the confidentiality, integrity, or availability of data or IT systems (RCW 42.56.420 (4)).

- **Category 4 – Confidential Information Requiring Special Handling:** confidential information requiring special handling is information that is specifically protected from disclosure by law and for which especially strict handling requirements are dictated through statute, regulation, or agreement and serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions. This information includes, but is not limited to:
  - Any information about an individual’s medical history, mental or physical condition, or about a health care professional's medical diagnosis or treatment of the individual, must be secured in a separate location (physical or electronic) and access must be restricted to individuals who explicitly require access to the information for agency business (see storage and sharing below);
  - Wage data obtained through state unemployment insurance records must be secured in a separate location (physical or electronic) and access must be restricted to individuals who explicitly require access to the information for agency business (see storage and sharing below);

- **Secured data:** Data encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person ((RCW 42.46.590(11)).
- **Security breach:** Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of confidential information maintained by an agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure ((RCW 19.255.005(1) & RCW 42.46.590(9)).
- **Trusted network:** a network that includes security controls. At a minimum, these controls must include a firewall, access control on networking devices such as routers or switches, and antimalware software (including antivirus). Trusted networks may also include other mechanisms which protect the confidentiality, integrity, and availability of data.

3. Security Requirements

This section describes the data security requirements for Information Technology (IT) services procured by the SWC.

a. **Scope** – this section covers all information owned or in the possession of the SWC and information systems and resources used for the collection, processing, use, sharing, maintenance, dissemination, or disposition of information, whether digital or non-digital. Information includes physical and electronic records. Information systems and resources include personnel, equipment, and information technology such as hardware, firmware, and software.

b. **Configuration and security controls** – IT providers contracted by the SWC must have the capability to limit access to information systems to authorized users and devices on an individual level. Specific controls include:

   i. **User account authorization and authentication**

      1. **Information security roles and responsibilities** – at a minimum, IT providers must segregate users into staff and administrator accounts with access restrictions as follows:

         a. **Staff** – provides general access to the SWC's network. Software installation or removal and access to system settings is restricted.

         b. **Administrator** – provides administrative access to the SWC's network. Software installation or removal and access to system settings is unrestricted.

      2. **Authentication, password creation, and password aging requirements**

         a. **Authentication** – IT providers contracted by the SWC must use an advanced encryption standard (AES) required for Federal information processing standards. Users must be authenticated through this process to access any data managed by the IT provider. Failed logon attempts must lock a user's account for a full minute after 10 failed attempts. An account being locked must automatically alert the IT provider and an authorized representative of the SWC.

         b. **Password creation and aging requirements –** creating or changing a password must be enforced by industry standard complex password requirements and must be changed every 90 days. The complex password requirements are as follows:

            - May not include the user's account name or any part of their full name.
            - Must contain characters from three of the following categories:
               - Uppercase letters,
               - Lowercase letters,
               - Numbers,
               - Special characters (such as: ! @ # $).
            - May not consist of a single dictionary word.
            - Must be significantly different from previous versions of passwords. For instance, changing a number within the password incrementally is not sufficiently different to meet this requirement.

   ii. **Configuration baselines** – Configuration baselines are documented sets of specifications for information systems or items within those systems. Baseline configurations ensure a minimum level of security and reduce the possibility of introducing new configurations that could lead to unwanted vulnerabilities. IT providers contracted by the SWC must develop configuration baselines for use in all current and future builds, releases, and changes to information systems, components, or network configurations. The IT provider, in consultation with the SWC, will create or modify baselines as organizational needs change over time. Specific baseline configurations are as follows:

      1. **Remote access** – Remote access to the network through VPN is required. VPN software utilized by the IT provider must be National Institute of Standards and Technology (NIST) validated, must encrypt all remote access traffic based on FIPS 140-2 encryption standards, and utilize multi-factor authentication.

      2. **Portable devices** – Portable devices, such as laptops and tablets, must be configured to automatically lock after a period of inactivity of no more than 20 minutes.

3. **Software installation restriction** – automated network security protocols must be in place to prevent any unauthorized installations of software.
4. **Anti-malware software** – All devices, as appropriate, must have anti-malware software installed with current threat definitions.

c. **Return, reuse, and disposal** – all equipment containing information system media are subject to return, reuse, and disposal requirements. Equipment containing information system media includes, but is not limited to, scanners, copiers, printers, notebook computers, workstations, servers, network components, and mobile devices.

i. **Equipment reuse** – equipment containing information system media may be reused after clearing or purging the information contained on the device.

ii. **Equipment disposal** – all equipment containing information system media is subject to disposal requirements, including but not limited to scanners, copiers, printers, notebook computers, workstations, servers, network components, and mobile devices. Disposal of any equipment that contains information system media must include a sanitation process that removes information from the media in a way that such information cannot be retrieved or reconstructed.

1. **Disposal of storage devices containing only category 1 or category 2 information** – Equipment that includes data containing only category 1 or category 2 information, may be disposed of or recycled after clearing or purging the information contained on the device.
2. **Disposal of storage devices containing category 3 or category 4 information** – portable hard drives or hard drives in equipment such as notebook computers, workstations, servers, or mobile devices, that include data containing category 3 or category 4 information, must be disposed of by one of the following methods:
    a. Sanitization by an industry-standard data sanitation method, such as Secure Erase, Random Data, or Write Zero, that ensures information cannot be retrieved or reconstructed; or
    b. Physical destruction of the device that prevents operation or reconstruction.
3. **Disposal of optical storage devices** – due to security risks, the SWC authorizes only category 1 and category 2 information to be stored on optical storage mediums, such as compact disks (CDs), digital versatile disks (DVDs), and Blu-ray disks (BDs). Optical storage mediums may be disposed of by physical destruction.
4. **Disposal of peripheral devices with flash memory** – printers, scanners, multi-function copier devices, and network components with flash memory storage must have the memory storage cleared before disposal.

d. **System maintenance and protection** – the following maintenance and protection protocols must be put in place to prevent the compromise of the network or other data systems necessary for operations.

i. Maintenance of SWC information systems to ensure they are in tune with the requirements of users, data processing standards, and Federal or state government laws and regulations. This includes, but is not limited to:

1. Corrective maintenance arising from software errors, hardware failure, or inability to meet system performance needs;
2. Adaptive maintenance necessary for changes in data environments, processing needs, or changes involving hardware or systems software;
3. Perfective maintenance to improve processing efficiency, performance of applications, or user experiences.

ii. All software security patches or hotfixes for any software used must be applied within 3 months of being made available, unless clear evidence is presented that doing so will compromise the security, integrity, or availability of data.

e. **Backup operations and disaster recovery** – the following backup and disaster recovery protocols must be put in place to ensure the availability of data:

i. File server backups must be performed and stored every hour on a backup server. Each day a backup covering the previous 24 hours must be scanned for integrity and saved to a secure server hosted by the IT provider. All backups must be encrypted using cryptographic modules that are compliant with Federal Information Processing Standards (FIPS) and that are validated by the National Institute of Standards and Technology (NIST).

ii. Backup files must be retained as follows:

1. Hourly backup - 7 days;
2. Daily backup - 35 days;
3. Monthly backups must be kept indefinitely contingent upon available server space. The IT provider will notify the SWC when the server is close to running out of space. When this occurs, backup files must be archived to physical media or destroyed based on retention requirements associated with the data contained within.

f. **Security breaches**

i. **Response** – in the event the IT provider discovers unauthorized data acquisition that compromises the security, confidentiality, or integrity of information maintained by the IT provider, the IT provider must:

1. Immediately notify the SWC;
2. Conduct a risk assessment immediately following discovery of the data breach in order to identify the scope of the breach and any possible root cause(s);
3. In the event where any personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, assist the SWC in providing required notification to those affected.

4. References

- RCW 9.35.020 (identify theft law)
- RCW 19.255.005 (business regulations – personal information – definitions)
- RCW 19.255.010 (business regulations – personal information – notification of security breaches)
- RCW 42.56.420 (4) (public officers and agencies – public records act – information about the infrastructure and security of computer and telecommunication networks)
- RCW 42.56.590 (public officers and agencies – public records act – personal information – notification of security breaches)
- Office of the Chief Information Officer (OCIO) Policy 141.10
- TEGL 39-11 (protection of PII)
- FIPS 199 (standards for security categorization of federal information and information systems)