DATA SECURITY INCIDENT AND BREACH POLICY

Policy Number: 3030 **Effective Date:** March 26, 2021

OVERVIEW

Data breaches are increasingly common occurrences whether caused through human error or malicious intent. Workforce Snohomish (WFS) operations rely on the proper use of Confidential Information (CI) and Personally Identifiable Information (PII) on a daily basis. Managing risk and responding in an organized way to Incidents and breaches is key to operations and required by Washington state law.

PURPOSE

WFS must have a robust and systematic process for responding to reported data security Incidents and breaches. This policy is designed to standardize the WFS response to any reported Breach or Incident and ensure that they are appropriately logged and managed in accordance with Washington state law. Standardized processes and procedures help to ensure WFS can act responsibly, respond effectively, and protect its information assets to the extent possible.

GENERAL INFORMATION

Data Security Incident

A “Data Security Incident” or “Incident’ shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources managed by WFS.

Common examples of data security Incidents include, but are not limited to, any of the following:

1. Successful attempts to gain unauthorized access to a WFS system or Staff or Client PII regardless of where such information is located
2. Unwanted disruption or denial of service
3. The unauthorized use of a WFS system for the processing or storage of Confidential Information or PII

Workforce Snohomish

4. Changes to WFS system hardware, firmware, or software characteristics without the WFS's knowledge, instruction, or consent
5. Loss or theft of equipment where Confidential Information or PII is stored
6. Unforeseen circumstances such as a fire or flood that could lead to the loss or misuse of Confidential Information or PII
7. Human error involving the loss or mistaken transmission of Confidential Information or PII
8. Hacking, social engineering, phishing or other subversive attacks where information is obtained by deceitful practice

Data Security Breach

A "Data Security Breach" or "Breach" is any Incident where WFS cannot put in place controls or act to reasonably prevent the misuse of Confidential Information or PII. A Breach is also an Incident where data has been misused.

Adopting a standardized and consistent approach to Incident management shall ensure that:

1. Incidents are reported in a timely manner and can be properly investigated
2. Incidents are handled by appropriately authorized and skilled personnel
3. Appropriate levels of management are involved in response management
4. Incidents are recorded and documented
5. Organizational impacts are understood and action is taken to prevent further damage
6. Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny
7. Incidents are dealt with in a timely manner and normal operations are restored
8. Incidents are reviewed to identify improvements in policies and procedures
9. For a data beach, external agencies, customers, and data users are informed within 30 calendar days of the breach being discovered. RCW 19.255.010 The notice must be written in plain language and include:
    a. WFS contact information; and
    b. A list of the personal information involved in the breach; and
    c. A timeframe for the exposure as a result of the breach; including the date when the breach was discovered; and
    d. The toll-free telephone numbers and addresses of major credit reporting agencies if the breach exposed PII

10. For a data breach involving the PII of more than 500 Washington residents, the Washington state Attorney General will be notified within 30 calendar days of the breach being discovered. This notice will include:
    a. The number or estimated number of Washington consumers affected by the breach; and
    b. A list of the personal information involved in the breach; and
    c. A timeframe for the exposure as a result of the breach, including the date when the breach was discovered; and
    d. A summary of steps taken to contain the breach; and
    e. A single sample copy of the security breach notification, excluding any personally identifiable information.

Incidents can occur locally, in the cloud, or through third party service providers. Reporting and management of Incidents shall occur similarly. Third party providers shall also be governed by contract terms and liability as defined in their operational agreements.

DATA CLASSIFICATIONS

Washington state law, RCW 19.255.005, defines the following data as PII and any breach involving this data should be handled as described in this policy.

Personal identifiable Information

First name or first initial and last name in combination with any one or more of the following data elements:

A. Social security number
B. Driver's license or Washington ID card number
C. Account or credit/debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
D. Full date of birth
E. Private key that is unique to an individual and is used to authenticate or sign an electronic record
F. Student, military or password identification number
G. Health insurance policy or ID number
H. Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or

Workforce Snohomish

a. 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;
b. Username or email address in combination with a password or security questions and answers that would permit access to an online account; and
c. Any of the data elements or any combination of the data elements described in (A-G) without the consumer's first name or first initial and last name if:
    i. Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and
    ii. The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.