5.10
About Data and Systems Access Policies

5.10.10 Purpose of these policies

September 5, 2014

The purpose of these policies is to define the conditions under which access to specific statewide systems, applications, and data will be granted.

5.10.15 Authority for these policies

July 1, 2012

RCW 43.88.160 (4) requires the Office of Financial Management (OFM) to develop and maintain a system of internal controls and internal audits comprising methods and procedures to be adopted by each agency that will safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies for accounting and financial controls.

The Public Records Act 42.56 RCW prohibits disclosure of certain personal and other information.

5.10.20 Related policies

July 1, 2012

The Office of Chief Information Officer (OCIO) Policy No. 141, *Securing Information Technology Assets*, sets requirements for maintaining system and network security, data integrity and confidentiality.

5.10.25 Who must comply with these policies?

July 1, 2012

All executive, legislative, or judicial branch agencies connecting to statewide systems must comply with the policies in this chapter.

5.10.30 Statewide systems, applications, and data covered under this policy

September 5, 2014

This policy covers access to certain statewide systems, applications, and data that the Department of Enterprise Services (DES) manages and maintains on behalf of OFM to carry out OFM's responsibilities described in the section "Authority for this policy." Systems, applications, and data covered include:

- IRS Form 1099-MISC Reporting System
- Enterprise Reporting Standard Reports (ER)
- Enterprise Reporting Web Intelligence (Webi)

5.10.35 Controls over systems, applications, and data covered under this policy

September 5, 2014

Agencies should have internal controls over granting and revoking access to systems, applications, and data that:

- Limit access to employees to only that necessary to perform the assigned duties.
- Consider how access will affect agency internal controls and apply compensating controls where necessary. Refer to Chapter 20.
- Ensure proper employee training under OCIO policies.
- Employ a systematic employee exit process that revokes access within a reasonably short amount of time after the employee's access is no longer required. This may happen when job duties change or when an employee leaves the agency.
- Allow for periodic review of all employees' statewide access.

5.10.40 Specific requirements

September 5, 2014

5.10.40.a **IRS form 1099-MISC Reporting System**

Agencies accessing the 1099 download maintained by the Department of Enterprise Services (DES) are required to comply with Subsection 50.10.65.

5.10.40.b **Enterprise Reporting Standard Reports (ER) and Web Intelligence (Webi)**

Agencies accessing the Enterprise Reporting Standard Reports (ER) or Web Intelligence (Webi) maintained by DES must establish an effective system for management and control of sensitive information as appropriate. In addition, access to vendor payment related data belonging to other agencies is restricted to employees who need the data to perform their assigned duties, and before access is granted:

1. An employee must sign a Non-Disclosure Agreement (NDA) that includes the following statements:

    - I will not access or use vendor payment information for any commercial or personal use or gain, but only to the extent necessary and for the purpose of performing my assigned duties as an employee.

    - I will not directly or indirectly disclose, divulge, transfer (such as but not limited to, email, portable media, File Transfer Protocol (FTP), file location services), release, communicate, sell, or otherwise make known to unauthorized persons or any third party outside the scope of my position any vendor payment information during duty hours as well as non-duty hours or when not in use unless authorized by my supervisor, agency policy or applicable state law.

    - I will not duplicate or reproduce vendor payment information except for the purpose of performing my duties as an employee.

    - I will protect vendor payment information from unauthorized physical and electronic access in a manner which prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.

    - I will dispose of vendor payment information, in electronic or paper form, in an appropriate manner.

    - I agree to abide by all federal and state laws, regulations, and policies regarding the safeguarding and disclosure of the information.

2. Agencies may use an alternate in-house NDA form provided written approval from OFM is obtained.

3. The agency security administrator must certify that that the employee has signed the non-disclosure agreement and needs access to other agency vendor payment related data to perform the employee's assigned job duties. In certain cases, OFM must approve the request before access can be granted.

To get access to Enterprise Reporting vendor payment related data for other agencies, follow the instructions and fill out the forms at: http://www.ofm.wa.gov/resources/dataaccess.asp.

If an agency detects a breach in security related to vendor payment related data, the agency is responsible to follow the steps for breach as described in RCW 42.56.590 and notify the Consolidated Technology Services (CTS) Chief Information Security Officer, CTS Security Operations Center and the Washington State Patrol Computer Crimes unit. Additionally, the agency is to notify DES within one business day of discovering the breach and take corrective action as soon as practicable to eliminate the cause of the breach. DES may request a full review of the agency's data security controls.