Agreed-Upon Procedures related to the Washington State Department of Licensing's Data Sharing Agreement

Introduction

The Department of Licensing (DOL) has worked with the Office of the Washington State Auditor (SAO) to develop the following agreed-upon procedures related to non-state governmental and private organizations' compliance with data security requirements of the DOL's Data Sharing Agreement.

These procedures were developed in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

The DOL has agreed to and acknowledged these procedures are sufficient for its purposes.

Intended Use

The DOL's Data Sharing Agreement requires a third-party "audit" of the engaging organization's policies, procedures and controls related to securing information technology systems, applications, and data. These procedures are made available for independent third-parties to use when conducting these required third-party "audits".

Please note, these procedures are **not intended to be used** for data sharing agreements in which the data security requirements specify "Data Security Requirements for State Agencies".

Agreed-Upon Procedures

1. Cybersecurity industry standards:

a) Inspect the organization's Administrative controls and document which industry standard is used to protect the environment(s) accessing, processing or holding Data.

Note: The industry standard identified in procedure 1a will determine which of the following standard-specific agreed-upon procedures should be applied. If the organization does not identify an industry standard in its Administrative controls document, the auditor should use the standard-specific procedures for OCIO 141.10. If the organization identifies different industry standards for different types of data, the auditor should use the standard(s) assigned to the environment(s) that access, process, hold or pass-through Data.

2. Network security:

a) Inspect the organization's Administrative controls to confirm an approval and testing process of firewall changes is required.

b) Inspect documentation to confirm the organization maintains a record of changes made to its firewall.

c) Ask IT personnel to confirm the last firewall change was approved and tested according to the Administrative Controls.

d) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Inspect the current firewall configuration to ensure the organization has blocked services, protocols and ports deemed unallowable by the organization (OCIO 141.10 §5.1.2).
- [ISO] Inspect a list of allowable network and network services allowed to be accessed through the firewall (ISO 27002:22 §8.21).
- [NIST] Ask IT personnel whether any connections (such as backup internet connections) to an external network do not go through a firewall or some other security boundary device (NIST 800 SC-7).
- [PCI] Inspect the current firewall configuration to ensure the organization has blocked services, protocols and ports deemed unallowable by the organization (PCI-DSS §1.4.2).

e) Inspect the organization's intrusion detection and prevention systems configurations to confirm intrusion-detection and/or intrusion-prevention techniques are configured, maintained and updated timely.

f) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Inspect the organization's documentation of its periodic review of intrusion detection and prevention system logs (OCIO 141.10 §10.3).
- [ISO] Identify the monitoring tool used and confirm the tool monitors continuously (i.e., alerts) (ISO 27002:22 §8.16).
- [NIST] Identify the monitoring tool the organization uses and confirm it is configured to detect attacks and unauthorized connections (NIST 800 SI-4).
- [PCI] Identify the monitoring tool the organization uses and confirm it is configured to detect attacks and unauthorized connections to the cardholder data environment (PCI-DSS §11.5.1).

g) Inspect evidence to confirm the organization performed vulnerability assessments and scans designed to expose potential vulnerabilities on external and internal network devices and servers.

h) Select one scan report from each of the last four quarters. Inspect each to confirm the organization remediated or has a documented plan in place to address all vulnerabilities ranked "high" or above. For these vulnerabilities, confirm the organization completed re-scans that show no pre-existing vulnerabilities ranked "high" or above remained.

i) Confirm the annual penetration test was performed by a qualified, external, third–party vendor in the past year.

j) Inspect the scope of work and results from the most recent external penetration test to confirm testing was performed in the past year and after any significant changes to the IT environment. Examples of significant changes include a new operating system, installation of new hardware on the network, or rollout of new, commercial, off-the-shelf software.

k) Select one vulnerability with severity ranking less than "high" and inspect documentation to confirm the organization has planned, and is tracking, corrective action in accordance to its severity.

l) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Confirm for up to five systems using or accessing Data, that the organization re-evaluated its related IT Risk Assessments in the last three years (2023 OCIO).
- [ISO] Inspect a list of assets subject to the vulnerability scans. Ask IT personnel what controls are in place to confirm the list is accurate (ISO 27002:22 §8.8).

- [NIST] Confirm the organization incorporated the results of the latest scan in its current IT Risk Assessments (NIST 800 CA-8 and RA-5).
- [PCI] If internal personnel performed the penetration test referred to in procedure 2(i), inspect IT management's documentation demonstrating that those employees met necessary qualifications (PCI-DSS §11.3.1 and §11.4.3).

3. Access Security:

a) Inspect configuration settings for one system processing Data and confirm whether:
   - The organization assigns a unique ID for each user, and
   - A complex password is required.

b) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]
   - [OCIO] Inspect configuration settings for one system using, accessing or processing Data and confirm whether or not it permits the re-use of any of the last four previous passwords (OCIO 141.10 §6.1.2, §6.2 and §6.3.1.4).
   - [ISO] Inspect configuration settings for one system using, accessing or processing data and confirm whether or not it permits re-use of any previous passwords (ISO 27002:22 §5.17).
   - [NIST] Confirm the organization's Administrative controls address notification requirements for personnel changes (terminated, transferred or changed positions) that affect user roles (NIST 800 AC-2).
   - [PCI] Ask IT managers about their examinations of audit logs and how they confirm each user ID is associated with an individual (PCI-DSS §8.2).
   - [PCI] Confirm that audit logs for one system using, accessing or processing Data identify specific user IDs (PCI-DSS §8.2).

c) Inspect configuration settings for one system using, accessing or processing Data and confirm whether users must change passwords at least once every 90 days.

d) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]
   - [OCIO] Inspect configuration settings for one system using, accessing or processing data and confirm whether or not it permits passwords that contain the username, user ID or any form of the user's full name (OCIO 141.10 §6.3).
   - [ISO] Confirm the organization's Administrative controls address stricter requirements for enforcing password changes, beyond standard timeframe requirements (for example, after a security incident). (ISO 27002:22 §5.17).
   - [NIST] Confirm the organization's Administrative controls address stricter requirements for re-authentication (for example, after a security incident.) (NIST 800 IA-5 and IA-11).
   - [PCI – No additional procedure required.]

e) Ask IT personnel whether or not controls exist that require user authentication when using, accessing or processing Data (for example, multi-factor authentication).

f) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Ask IT personnel whether the process for setting up new users requires that users change their password from an assigned password immediately (OCIO 141.10 §6.1.2).
- [ISO] Ask IT managers whether there are any shared identities, for administrative or other reasons, that can access Data (ISO 27002:22 §5.16).
- [NIST] Confirm the organization has a list of account managers authorized to approve new user accounts (NIST 800 AC-2).
- [PCI - No additional procedure required]

4. Application Security:

a) Inspect the organization's Administrative controls and confirm they define a timeline to install patches, upgrades, updates, and bug fixes for vulnerabilities classified as "high" or above, after they have been released.

b) Obtain reports or logs of patches, upgrades, updates and bug fixes released during the last 12 months. From each of the past four quarters, select one security patch, upgrade, update or bug fix and:

- Document when each patch was installed.
- Confirm whether each was installed within the timeframe defined in the Administrative controls.

c) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Confirm the last patch, upgrade, update or bug fix was installed after testing was completed and approved (OCIO 141.10 §7.3).
- [ISO] Ask IT personnel how they deem patch, upgrade and bug fix tests were successful before being released to live environment (ISO 27002:22 §8.19).
- [NIST] Confirm the last firmware or software update was installed after testing was completed and approved (NIST 800 Sl-2).
- [PCI] Confirm the organization's Administrative controls defines the timeline for critical or high-security patches/updates as "within one month" (PCI-DSS §6.3.3 V4.0).

d) Confirm the organization retains a list of all web-based applications using, accessing or processing Data.

e) Inspect the organization's Administrative controls specific to web-based software application development and ask IT personnel responsible for code change review to confirm that:

i. All custom application code changes are reviewed by another IT staff member before they are moved to the live environment.

ii. Code changes are reviewed by someone who is not the originating code author, and by people trained or experienced in code-review techniques and secure coding practices.

iii. Appropriate corrections are implemented before code changes are moved to the live environment.

iv. Personnel responsible for each application has reviewed and approved code-review results before code changes are moved to the live environment.

v. Code changes are coded according to Open Web Application Security Project (OWASP) or SysAdmin, Audit, Network and Security (SANS) guidance.

f) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Ask IT personnel how the organization evaluated the security impact code change for the last change (OCIO 141.10 §7.4).
- [ISO] Confirm the organization maintains a list of web-based software applications that are supported by third-party vendors (ISO 27002:22 §8.25 and §8.28).
- [ISO] Ask IT managers what methods are used to obtain assurance the web-based software supplier complies with the organization's rules for secure development (ISO 27002:22 §8.25 and §8.28).
- [NIST] Ask IT managers what tools or controls are in place to detect and eradicate malicious code in their web-based software (NIST 800 Sl-3).
- [PCI] Obtain documentation of the last code change to a web-based software and confirm there was segregation of duties for development, testing, review and approval before it was released to the live environment (PCI-DSS §6.2.3.1).

5. Computer Security:

a) Inspect the organization's Administrative controls related to patch installation for all computer operating systems and confirm the patching process requires no less than monthly updates/patches for vulnerabilities classified as "high" or above.

b) Confirm the last critical security patch was installed within the lesser of 30 days or the timeframe stated in the organization's Administrative Controls.

c) Obtain a list of patches from the last 12 months. Select one security patch that was not pushed within 30 days and ask how IT managers determined it was non-critical. Confirm the patch was installed within the timeframe defined by the Administrative Controls for non-critical vulnerabilities.

d) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Confirm the organization's Administrative Controls require computer patches be tested before deployment to the production network (OCIO 141.10 §5.5).
- [ISO] Confirm the organization maintains an audit log of all updates to operational software (ISO 27002:22 §8.19).
- [NIST] Confirm what system maintenance tools, or compensating controls, the organization uses to monitor computer security (NIST 800 MA-3).
- [PCI] Confirm the last critical security patch tested in 5c was the last critical patch identified by the vendor (PCI-DSS §6.2).

e) Inspect the organization's Administrative controls and confirm they require anti-malware software and definitions be kept up-to-date for all computer systems.

f) Inspect anti–malware configurations to confirm anti-malware programs:

i. Detect all known types of malicious software.
ii. Remove all known types of malicious software.
iii. Protect against all known types of malicious software.
iv. Have log generation enabled.
v. Are current and up to date. Anti-malware programs should be updated weekly, at a minimum.

g) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Ask IT personnel whether anti-malware programs extend to file transfers, email and web browser-based traffic. If not, ask what compensating controls are in place related to those options (OCIO 141.10 §5.7).
- [ISO] Ask IT personnel:
    - How downloads and attachments to emails and instant messaging are scanned for malware before use or when accessed (ISO 27002:2 §8.7).
    - Whether these scans are done when entering network and/or at different places of interception (ISO 27002:2 §8.7).
- [NIST] Ask IT personnel whether periodic scans are performed on systems, and real-time scans are performed on files from external sources. Confirm this aligns with the organization's Administrative Controls (NIST 800 SC-35 Sl-3).
- [PCI - No additional procedure required]

6. Data Storage:
Note: DOL Data is not permitted to be saved on medium storage; however, organizations may opt for stricter controls and guidance.

a) Confirm the organization maintains a list of all computing equipment storing, accessing, processing, or using Data.

b) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Inspect the organization's inventory of information and associated assets and confirm it identifies responsible personnel for each asset (OCIO141.10 §8.2).
- [ISO] Confirm the organization updated its inventory of information and associated assets within the last three years (ISO 27002:22 §5.9).
- [NIST]
    - Confirm the organization's inventory of information and associated assets identifies responsible personnel for each asset and other necessary tracking elements (for example, location) (NIST 800 CM-8 and CM-13).
    - Confirm the organization updated its inventory of information and associated assets within the last three years (NIST 800 CM-8 and CM-13).
- [PCI] Confirm the list obtained in 6a was updated within the last three years (PCI-DSS §12.5.1).

c) Through observation or inspection, confirm the organization has controls to prevent transferring Data onto portable media.

d) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Inspect the organization's Administration controls to confirm when medium storage is or is not permitted for confidential data (OCIO 141.10 §5.8).
- [ISO] Confirm the organization's Administrative controls identify classification categories of information (ISO 27002:22 §8.12).
- [ISO] Ask IT managers which monitoring tools or controls are in place for data channels (for example, email and file transfers) (ISO 27002:22 §8.12).

- [ISO] Ask IT personnel how downloads and attachments to emails and instant messaging are scanned for malware before use or when accessed (ISO 27002:22 §8.12).
- [ISO] Ask IT personnel whether these scans are done when entering network and/or at different places of interception (ISO 27002:22 §8.12).
- [NIST] Inspect the organization's Administration controls to confirm when medium storage is or is not permitted (NIST 800 MP-7).
- [PCI - No additional procedure required]

7. Electronic Data Transmission:

a) Ask IT managers whether protected personal information (PPI) is transmitted to DOL or exchanged with recipients. If yes, inspect up to five transmission systems (for example, email or secure file transfer) configurations to confirm transmission uses a strong encryption method for secure transmission.

b) Select up to five web-based systems, transferring any level of data, and confirm:

i. Hypertext Transfer Protocol Secure (HTTPS) is displayed on the web browser's Uniform Resource Locator (URL) through inspection.

ii. The score or results of the server configuration by using SSL Lab's tool or a similar product.

c) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] If the organization transmits any PPI, confirm the encryption used ties to NIST FIPS standard for both data at rest and in transit (2023 OCIO).
- [ISO] Ask IT personnel how access to Data is tracked and logged (ISO 27002:22 §8.3).
- [ISO] Ask IT personnel how access to Data is limited to only business needs (ISO 27002:22 §8.3).
- [NIST - No additional procedure required.]
- [PCI] Inspect the organization's Administrative controls and confirm procedures ensure (PCI-DSS §4.2.1 §40):
    - Only trusted keys and certificates are accepted.
    - Transmission over open networks use certificates.
    - Tools used are kept up to date.
    - Encryption strength is relevant to data classification.

8. Data at Rest:

a) Obtain the organization's list of all equipment that stores, accesses, processes or uses Data. From the list, select:

i. One primary server, CPU, etc., and confirm it uses a strong encryption method.

ii. One backup of a server, CPU, etc., and confirm it uses a strong encryption method.

b) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO - No additional procedure required]
- [ISO] Ask IT managers to describe the processes used to determine the level of protections based on data sensitivity (ISO 27002:22 §8.11 and §8.24).

- [NIST] Ask IT managers whether the organization has controls that align encryption strength to data classification for data at rest (NIST 800 SC-13 and SC-28).
- [PCI] Ask IT personnel what tools are used regarding the storage of secret and private keys (PCI-DSS §3.5.3).

9. Data Minimization:

a) Inspect the organization's Administrative controls regarding periodic data clearing and destruction. Confirm it covers all media types that access, process or use PPI, and defines requirements for certifying disposal processes are completed within the prescribed time listed in the contract for each of the following:

- Once Data is no longer needed for business purposes; and
- At the expiration of the required retention period by law or standard.

b) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO - No procedure required]
- [ISO] Inspect the organization's Administrative controls and confirm retention schedules are supported by legal compliance requirements (ISO 21002:22 §5.33 and §5.34).
- [NIST - No procedure required]
- [PCI] Inspect the organization's Administrative controls and confirm retention schedules are supported by legal compliance requirements (PCI-DSS §3.2.1).

10. Data and Media Sanitization:

a) Confirm the organization's Administrative controls:

- Require sanitization procedures prior to disposal, surplus or reuse.
- Align with sanitization mechanisms (clear, purge or destroy) based on classification of information. (NIST SP 800-88 §2.5-2.7)

Notes: The organization may have a DOL-approved waiver to the destruction requirement, or DOL contract personnel may have provided a specific disposal requirement. If not, the organization must have a practice of:

(1) preventing simple non-invasive data recovery (aligns with clear),
(2) rendering the target data unrecoverable using state-of-art techniques (aligns with purge), or
(3) making the media no longer usable (aligns with destroy).

b) Inspect the organization's documentation of the last disposal of PPI, or its equivalent, and confirm the destruction method used followed the Administrative controls procedures.

c) [***Instructions:*** *Select the appropriate agreed-upon procedure based on the standard identified in procedure 1(a). Delete those that do not apply.*]

- [OCIO] Inspect the organization's documentation of the most recent disposal of PPI, or an equivalent of confidentiality, in the last three years and confirm the results of the deletion was verified (OCIO 141.10 §8.3).
- [OCIO] If there has been no disposal of PPI within the last three years, ask IT personnel how media is physically secured until destruction (OCIO 141.10 §8.3).
- [ISO] Inspect the organization's documentation of the most recent disposal of PPI, or its

equivalent, in the last three years and confirm the results of the deletion was verified (ISO 2700:22 §8.10 and §7.14).

- [NIST] Ask IT personnel how system documentation regarding the disposal process is protected from unauthorized access (NIST 800 MP-6).
- [PCI] Ask IT personnel how the storage location of media is protected from unauthorized access until destruction (PCI-DSS §9.8).

11. Hardcopy Storage:

a) Obtain a list of all personnel, vendors and contractors who handle, store or transmit hardcopy Data, including the geographical locations where hardcopy data is handled or transported to.

b) Inspect the organization's Administrative controls regarding direct handling of Data in hardcopy form and confirm they follow DOL's Data Sharing Agreement requirements.

c) Ask at least one staff member who handle hardcopy Data whether Data is handled and stored in accordance with DOL's Data Sharing Agreement requirements.

12. Hardcopy Data Transportation:

a) Inspect the organization's Administrative controls regarding transporting hardcopy data with PPI and confirm they follow DOL's Data Sharing Agreement requirements.

b) Confirm the organization's most recent hardcopy data transportation records align with DOL's Data Sharing Agreement requirements for PPI transferred by:

i. Authorized personnel

ii. A courier

13. Offshoring – Electronic Records:

a) Obtain and confirm the organization maintains a list of all geographical locations where Data is accessed, processed or used by the organization, subrecipients or any third-party vendors.

b) For any offshore locations identified, confirm the organization has a DOL waiver or amended contract permitting the transmittal or access of Data from an offshore location.

14. Offshoring – Hard Copy:

a) Inspect the organization's Administrative controls regarding handling of Data in hardcopy form and confirm it does not permit hardcopies to be kept at locations outside of the United States.

b) If the organization does download or transfer hardcopies outside of the United States, inspect the DOL waiver or amended contract permitting the transfer of hardcopy of Data offshore.

15. Security Breach Notification:
Note: A security incident can include a lost USB drive or a missing paper file.

a) Inspect the organization's Incident Response plan and confirm it assigns responsibility for establishing, documenting and distributing security response and escalation procedures.

b) Inspect the Incident Response plan and confirm it provides direction to inform the designated DOL liaison of a breach.

c) Inspect the documentation from the most recent IT security incident in the last three years and

confirm it was handled in accordance with the organization's Incident Response plan.

d) If the organization had an IT security incident, but did not comply with its Incident Response plan, determine when the organization plans to respond to the situation. IT managers can work with their DOL liaison for any follow-up resolution.

DOL Definitions

Administrative controls: Written guidelines, policies or procedures to guide the behaviors and actions of the organization's personnel on matters pertaining to securing data.

> *Note: If an organization does not have its own policies related to an agreed-upon procedure because it outsources a service to a service provider (such as WaTech), the organization is expected to have written approval from its responsible official (whether departmental level or higher) that it is acceptable to rely on a service provider's policies related to that subject. If an organization has not made formal assessment of the service provider's policy and officially adopted it before the agreed-upon procedures engagement, then DOL considers that [the organization] does not have a policy in place.*

Personal protected information (PPI): Confidential information containing personal information and classified by the DOL as Category 3 or 4 data which would include DOL data (Data).

Strong encryption: The definition is based on PCMag.com
https://www.pcmag.com/encyclopedia/term/strong-encryption

IT managers and IT personnel: Auditors are expected to gain information and assurances from different levels of staffing involved in the process. IT managers are people with the appropriate knowledge of and decision-making authority over activities. IT personnel are typically those people responsible for performing the activities or having first-hand knowledge of the activities.

Additional Guidance

Outsourcing to a third-party vendor:

Organizations can outsource processes but not responsibilities to third-party vendors. For activities outsourced to a third-party vendor, the auditor must:

- Document the vendor's name.
- Confirm and document whether there is a current contract agreement between the organization/agency and the vendor.
- Identify and document whether the vendor obtains data from DOL directly or from another organization/agency.
  - Confirm a current data sharing agreement exists between the organization/agency and the vendor.

Penetration testing:

The intent of a penetration test is to simulate a real-world attack with a goal of identifying how far an attacker would be able to penetrate an environment. A penetration test differs from a vulnerability scan in that a penetration test is an active process that may include exploiting identified vulnerabilities. Read the following section for details.

Penetration Testing – Minimum Standard to comply with Data Security Requirements

The penetration test methodology needs to be based on industry-accepted penetration testing approaches. An example would be NIST SP800-115, however Open-Source Security Testing Methodology Manual

(OSSTMM), OWASP, and Penetration Testing Execution Standards (PTES) are a few of the other commonly accepted frameworks. If other approaches or frameworks are used, they must be identified in the engagement report; DOL may accept the approach or framework as technologies are always changing and a future solution not identified here may very well suffice to meet DOL's standard.

Penetration testing must cover all in-scope systems. In-scope would be all devices that handle, process, or store DOL's confidential information, and any system interacting with these systems. Examples include patching servers, domain controllers, and backup servers.

Penetration testing must be performed from both an internal and external perspective. To reduce cost to the entity having the penetration testing performed, DOL accepts providing the penetration testing team with the necessary information needed so the team can focus efforts on the appropriate systems.

Where segmentation is in use, testing must be performed to validate the effectiveness of the segmentation. The scope of testing may include one or more segments.

Application penetration tests to include, at a minimum, testing for vulnerabilities based on Application Security requirements in the Data Security Requirements contained within the data sharing agreement.

Network penetration tests to include components that support network functions as well as operating systems.

A comprehensive report detailing the penetration tests performed and the results, which would include a list of vulnerabilities identified with severity ranking on the affected host/system.

Some vendors will allow an organization to remediate identified vulnerabilities and document or update this in the report to achieve what could be considered a 'passing' final report. If this is not done, DOL will look to see the organization took appropriate actions to correct or reduce the risk rankings to an acceptable level before closing its review of the audit. This could be done over time but will need to be tracked as part of a corrective action plan to correct all deficiencies noted in the engagement report.