Managing Data Security and Privacy When Teleworking

University Standards: STN-U5410.02B

Effective: May 1, 2024

Authority

POL-U5410.02	Managing Telework Arrangements

See Also

FRM-U5346.01A	Remote Work Equipment Agreement Form
POL-U3000.07	Securing Information Systems
POL-U5315.02	Affording Individual Privacy Rights
POL-U3000.03	Training for End User Information Security Awareness
POL-U3000.02	Using Electronic Methods for University Communications
POL-U1600.07	Ensuring Accessible Technology Information
POL-U1500.08	Using University Resources Policy
SEC-08-01-S	Washington State Data Classification Standard

Application

These standards apply to all classified and professional staff, including temporary and non-permanent staff, and student employees who have an approved telework arrangement.

Purpose of Standards

Universities are a growing target for cybersecurity attacks and subject to an increasing number of privacy and information security regulations. The purpose of these standards is to educate employees and department heads on their responsibilities in assisting the University in ensuring compliance with privacy and information security requirements and to mitigate the increased risk to University data created by teleworking.

Oversight Responsibility

Vice Provost for Information Technology/Chief Information Officer

University Compliance Officer/University Privacy Program Coordinator

Definitions

Confidential Data

Any data that meets Category 3 or 4 per the Washington State security Data Classification Standard and is data specifically protected from release or disclosure by law such as, but **not limited to**, personal information as defined in RCW 42.56.590 and information about the infrastructure and security of computer and telecommunication networks as defined in

RCW 42.56.420. Confidential data also includes any data for which serious consequences could arise from unauthorized disclosure such as such as threats to health and safety, or legal sanctions. See the Washington State's Data Classification Standard for details.

Required Standards

1. **Employees are Required to Follow Safe Data Practices**

   Teleworking creates new risks in maintaining data privacy and information security. Employees are therefore required to maintain safe data practices as outlined in these standards to establish a compliant and secure telework setting.

2. **Supervisors Must Understand Which Employees Handle Confidential Data**

   Each supervisor must be knowledgeable about what Confidential Data (see definitions) each of their employees' access and handle while performing their job duties to ensure appropriate controls are in place for a telework arrangement. Supervisors and employees should consult with the Information Security Office if there are questions about data types, data handling and the telework setup.

3. **All Employees Must Complete Information Security Training Annually**

   All employees are required to complete annual Information Security Awareness Training per the *Training for End User Information Security Awareness Policy (POL-U3000.03).* A telework arrangement is not to be approved or renewed until the training is complete.

4. **Only University Owned and Managed Devices May be Used to Conduct University Business**

   All fully remote and hybrid employees must use a University issued and managed device (computer, laptop) to access, process, use, or share such data from their alternate work site. Managed devices are part of an Information Technology Services (ITS) configuration management system. Using personal computers to conduct University business elevates information security and privacy risks for the University.

   Exceptions:

   a) Employees who have not yet been issued a University computer for their telework site will be granted an exception via the *Remote Work Equipment Agreement eForm* until a University computer can be provided.

   b) Student employees whose duties involve accessing confidential data are not permitted to use a personal device to perform their job duties.

5. Use of Personal Cell Phones to Conduct University Business Permitted Under Certain Conditions

Use of personal cell phones may be used to conduct University business that involves access to University systems and applications, however:

a) Duration and frequency of use must be limited to only when it is necessary (i.e., when a University device is not readily available).

b) The phone is encrypted (when applicable) and password protected.

6. Employees Required to Submit Equipment Agreement for Teleworking

Each employee approved for a telework arrangement must submit an *Remote Work Equipment Agreement eform* to document the University property that is or will be used at the employee Alternate Worksite including devices. Employees are to resubmit a new agreement when the status of equipment changes.

Financial Managers must ensure University assets are tracked and returned in accordance with Section 11 of the *Managing Telework Arrangements Policy*.

7. University Device(s) Must be Encrypted

If approved for telework, employees must verify that their device is encrypted. See Device Encryption Verification Instructions.

8. Conducting University Business Through Personal Email Accounts is Prohibited

University business is not to be conducted through personal email accounts (i.e., gmail.com) in accordance with the *Using Electronic Methods for University Communications Policy (POL-U3000.02).* Using a personal email account to share Confidential Data is a significant security risk and violation of University policy.

9. Use of Unsecured Wireless Connections Prohibited

Employees are required to maintain their home networks securely, including requiring authentication (i.e., password protected) and encryption on wireless networks.

If employees are not at their Official Workstation, and are working on insecure networks (e.g., public wireless), they must use Western's virtual private network (VPN). ATUS provides support for using the University VPN.

10. Documents Containing Confidential Data Must be Stored in Authorized Locations

University documents belong to the state and must be stored only in authorized locations. Electronically maintained documents with Confidential Data are to be stored in:

a) Western's Microsoft 365 environment (e.g., OneDrive, SharePoint, Teams), and

b) University managed systems such as Banner, Canvas, or PageUp.

Employees are not permitted to store electronic documents containing Confidential Data on:

c) Hard drives of personal devices,

d) Removable media such as external hard drives, DVDs, phones, tablets, or USB thumb drives, or

e) Personal storage accounts including, but not limited to, Google, Box, Dropbox, or Office 365.

f) The University managed Google Drives and Docs environment,

g) Unencrypted hard drives of University owned and managed devices, and

h) Any applications that have not undergone a security design review by the Information Security Office. Email InformationSecurity@wwu.edu if unsure about a specific application.

Employees are encouraged not to print and/or store hard copy documents containing Confidential Data at their telework site. If necessary, such documents are to be secured in a manner that restricts unauthorized individuals from viewing or accessing (e.g., locked file cabinet) and kept separate from the employee's personal documents.

11. Only Employees are Authorized to Use University Devices and University Accounts

Allowing non-employees (including family members or roommates) to use University devices or have access to University accounts (i.e., Zoom and Teams) violates state ethics and privacy laws and substantially increases risk to the University. See also *Using University Resources Policy (POL-U5940.01).*

Employees must ensure that screens are locked, or systems are powered down before leaving a device unattended. Authentication will be required to unlock or logon to a device. University devices used off-campus and not in the employee's home must be under the employee's control or placed in a secure location at all times.

12. Privacy Protocols Must be Implemented at the Employee's Alternate Worksite

Employees with a telework arrangement are to implement sufficient protocols at their Alternate Worksite to ensure protection of individual privacy. Examples of protocol include, but are not limited to:

a) Conducting meetings in a private room and putting a "do not disturb" sign on the door,

b) Using a headset to reduce the amount of information others may overhear,

c) Not leaving hard copy paperwork containing private information where it may be accessible to others,

d) Disposing of paperwork appropriately (i.e., using a shredder not a waste basket),

e) Not discussing confidential or sensitive information with or around those who do not have a need or right to know,

f) Not conducting remote work in a public location, and

g) Preventing monitors/screens to be seen by others at the Alternate Worksite.

13. Exceptions May be Approved

If the remote work environment makes compliance with these standards difficult employee's and their supervisors must receive approval from the appropriate compliance and/or privacy owner to obtain a written exception to University policy or procedure and document any deviations from internal controls. For questions on who the appropriate compliance owner, contact the University Compliance Officer.

14. Employees to Promptly Report Security and/or Privacy Incidents

The University must promptly investigate data security and privacy incidents in order to manage risks and comply breach reporting requirements when applicable. Therefore, employees must promptly report all data security and privacy incidents to the employee's supervisor and the ATUS Help Desk.