SECURITY 101

OFFICE OF THE CISO
UNIVERSITY *of* WASHINGTON

SMART COMPUTING PRACTICES

ONLINE TRAINING
ciso.uw.edu/education/online-training/#security101

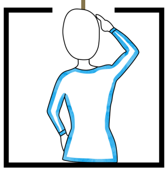
APS 2.4
washington.edu/admin/rules/policies/APS/02.04

1 KNOW YOUR DATA CLASSIFICATION

Data is classified as UW **Confidential**, **Restricted**, or **Public**. It is important to understand the distinctions between the data types and secure data accordingly. UW Administrative Policy Statement (APS) 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions defines these data types.

KNOW YOUR ACCESS PRIVILEGES 2

Once you determine what types of data you have you may want to consider who should have access to it. UW APS 2.4 refers to "**principle of least privilege**," which means that UW data, information, and information systems should be accessed only on a need-to-know basis.

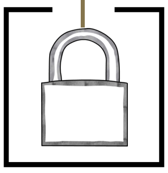


3 KNOW WHAT THE RISKS & THREATS ARE

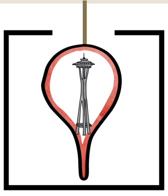
One of the most common threats to your personal and UW institutional data is **phishing**. Phishing is a form of Internet fraud in which cyber criminals send emails to entice victims into inadvertently surrendering confidential information. Cyberthieves can sell credentials and other valuable data on underground market places. "**Hacktivists**" can use stolen credentials to deface public-facing content on UW websites.

KNOW THE METHODS OF ENCRYPTING DATA 4

Encryption is the process of encoding either data or communications so that only authorized parties can access it. There are multiple ways to use encryption with digital communications for **data at rest**: individual files and folders may be encrypted, and so can hard drives, mobile devices, and other types of data storage. For **data in transit**, encryption can be used for email, network, Internet and wireless communications.



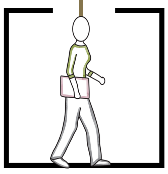
5 KNOW WHERE YOUR DATA IS STORED



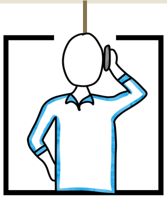
Know where your data is stored and **lock it up**. This includes desktop computers, mobile devices, portable storage devices, and in browsers, applications and paper filing cabinets. Refer to the Security 101 training link at the top for more information.

KNOW HOW TO SECURE YOUR DATA 6

Update & patch, use anti-virus software, limit administrative account usage, employ strong passwords & pins, use **multi-factor authentication**, encrypt whenever possible, use **eduroam** (encrypted wireless service), use **HuskyOnNet** (free encrypted VPN service), back data up, and wipe data from devices when you dispose of them.



7 REPORT INCIDENTS PROMPTLY



Who you report the incident to depends on the types of data involved.
If you are unsure about which types of data are involved, contact the **UW Office of the Chief Information Security Office**r at **ciso@uw.edu** or call **(206) 685-0116** for assistance.

CONTACT

Email: ciso@uw.edu | Phone: 206-685-0116