INFORMATION TECHNOLOGY
UNIVERSITY of WASHINGTON | TACOMA

University of Washington Tacoma Policy for Storage and Security of Data

The nature of campus data determines what measures and operational practices need to be applied to protect it. To help clarify the various minimum requirements for UW data security, categories of data have been classified as Public, Restricted, and Confidential (https://privacy.uw.edu/design/data-classifications/).

All restricted / confidential data of UW Tacoma should be stored to the UW Tacoma campus network or a UW approved cloud storage. In the event that unusual operational circumstances arise and there is a need to store restricted /confidential data to locations other that the UW Tacoma campus network or a UW approved cloud storage, the need and legitimacy must be reviewed and authorized by the Deans / department heads. A potential or confirmed breach must be reported as outlined in the University of Washington administrative policy https://www.washington.edu/admin/rules/policies/APS/02.05.html

UW Tacoma Information Technology can assist in reviewing and verifying devices and storage methods as well as installing encryption software to ensure they meet the data security standards of the University of Washington administrative policy.

Faculty and employees storing any data to the desktop hard drives (i.e. C drive) and/or portable storage devices are to do so at your own risk. UW Tacoma Information Technology will not be able to retrieve data due to desktop hard drives / portable drives failure.