UW Data and Your Responsibilities

University of Washington employees depend on UW data to support coordination and collaboration, effective decision support, and efficient operations University-wide. Be mindful that UW data are owned by the UW, regardless of where they are created, managed, or stored (e.g. email, UW systems, Google or Microsoft cloud services, personal smartphones, iPads or other mobile computing devices).

As a UW employee, you are responsible for protecting UW data, such as student records, health information, financial data, and other forms of personally identifiable information. Part of your responsibility includes knowing the applicable APSes, standards and guidelines. Please see http://passcouncil.washington.edu/psg/ for a complete list.

For further information, please contact the following resources

Information security and privacy:
http://ciso.uw.edu/, email ciso@uw.edu, or phone 206-685-0116

Data management and use:
http://www.washington.edu/uwit/im/dmc/, or email dmc-support@uw.edu

UW-IT services (such as cloud computing or appropriate use of UW resources):
http://www.washington.edu/itconnect/policy/, email help@uw.edu, or phone 206-221-5000

Social Security Number (SSN) Data Security Framework

Overview

The University of Washington is committed to protecting the privacy and confidentiality of personal information related to students, faculty, staff, and other individuals associated with the University. The University recognizes the risk and impact that the improper disclosure of SSNs can have on individuals who have entrusted this information to the organization.

The University of Washington routinely collects Social Security Numbers (SSNs) in support of several federal requirements such as W-2 tax forms and student educational tax credit reporting. SSNs are considered confidential data according to the UW Administrative Policy Statement (APS) 2.2, University Privacy Policy. Unauthorized release of SSN (and other personally-identifiable information) by the UW exposes individuals to identity theft and fraud, and brings financial and reputational harm to the UW.

Everyone who is accountable for the management or use of SSN data must also become familiar with other university-wide and departmental policies and procedures related to records management and security, which are published separately.

More Information

For more information about policies, training, and Frequently Asked Questions (FAQs) in relation to the protection of SSN data, please see:

UW Resources for Safeguarding Social Security Numbers (SSNs) from the PASS Council

---

A New University Privacy Policy is Underway to Address Unsolicited Email

Here's an excerpt from the policy:

To avoid or reduce Internet fraud, University units, including, but not limited to education, research, patient care, and service areas (internal and external to the University), and University workforce members shall not:

- Send unsolicited email (where the recipient has not granted permission for the message to be sent) to individuals that asks them to reply with confidential information; and

- Send unsolicited emails to individuals that ask them to click embedded links to University web self-service transactions that require entry of confidential information.

Unsolicited email does not include email sent from a University unit, including, but not limited to education, research, patient care, and service areas (internal and external to the University), to individuals who receive services from, or have an ongoing relationship with, the unit.

The Office of the CISO has information about phishing risks and best practices: http://ciso.washington.edu/resources/risk-advisories/phishing