Electronic Data and Information Security Policy

SCOPE
All information residing on University servers, desktops, laptops, and storage devices.

POLICY STATEMENT
University faculty, staff, students, volunteers or vendors who have access to Washington Technology University information described in this policy are expected to exercise discretion, common sense and reasonable judgment in connection with their use of information created, stored, transmitted or disposed in the course of their job duties, regardless of the medium in which that information is maintained. This includes the following:

- Personal information collected from and about students, faculty, staff, donors, business partners and others affiliated with the University
- Information relating to the core business practices of the university, including certain financial, legal, and operational information
- Other information relating to University operations that may be of a sensitive nature

Washington Technology University follows government regulations, including FERPA, to protect the privacy of students, faculty, and staff information. The data covered by this policy includes, but is not limited to, all electronic information found in e-mail, databases, applications and other media; paper information, such as hard copies of electronic data, employee files, and internal memos.

All members of the University community share in the responsibility for protecting information. Groups that have responsibility are as follows:

1. **Information Security Officer**: This person is responsible for monitoring compliance with the University Security Policies.
2. **Stewards**: Stewards are those members of the Washington Technology University community who have responsibility for particular university generated or maintained information and therefore, are responsible for the integrity of that data (for example, the Registrar's office for student transcripts). Stewards have a responsibility to use reasonable efforts to ensure that other individuals and third parties who receive such information understand their respective rights and responsibilities in using and transmitting the information to others. Joint stewards are mutually responsible for such information.
3. **Users**: All members of the University community are "Users" even if they do not have responsibility for managing resources. Users include students, faculty, staff, contractors, and volunteers. Users have the responsibility for protecting information resources to which they have access. Their responsibilities cover both computerized and non-computerized information and information technology devices (paper reports and records, books, film, microfiche, microfilm, computers

PDAs, disks, printers, phones, fax machines, etc.) that are in their care or possession. They shall follow the information security policies and procedures as well as any departmental or other specific applicable information security practices.

4. **Managers**: Managers are members of the University community who have management responsibility or supervisory responsibility, including deans, department heads, directors, supervisors, etc. Faculty who supervise teaching and assistants are included. Manager responsibilities include ensuring that their unit has completed education regarding information security, overseeing compliance with WTU policies and procedures in this regard, and immediately reporting breaches of this policy to the office of the CFO.

There are two main kinds of data covered under this policy:

1. University owned data that relates to such areas as financials, employment records, and payroll.
2. Private data that is the property of our students (past, present, and prospective) and/or employees, such as social security numbers, credit card information, and contact information.

DEFINITIONS

Public/Unclassified Information: Information that is generally available to anyone within or outside of the university. Access to this data is unrestricted, may already be available and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials and employee director information. Annual reports, tax returns, audited financial statements, and annual required Department of Education filings may also be available as public information but must be coordinated with the Office of the President.

Private/Confidential/Restricted Information: Information is defined as university information that is to be kept within the university. Access to this data may be limited to specific departments and cannot be publicly distributed. Private data includes, but is not limited to, employee and student personal information, certain policies, and other data as applicable. Examples of this type of data include social security numbers, tax forms, security procedures, employment data, business strategy information, trademark and patent data and other information as applicable.

POLICY

A. Data Classification

Washington Technology University data is to be comprised of two classifications: **Public/Unclassified Information** and **Private/Confidential/Restricted Information**. All information not otherwise classified as Public/Unclassified, will be assumed to be Private/Confidential/Restricted and may not be disclosed.

B. Access to and Control of Data and Information

1. Data is to be made available with sufficient granularity to allow the appropriate authorized access. There is a balance between protecting data and permitting access to those who need to use the data for authorized purposes.
2. Where possible and financially feasible, more than one person must have full rights to any University-owned server or cloud based system storing or transmitting high risk data. Data stewards may enact more restrictive policies for end-user access to their data.
3. Access to the network, cloud based systems, servers and systems should be achieved by the individual and unique logins and shall require authentication.

4. Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic or paper files or documents. All users must secure their username or account, password, and system access from unauthorized use.
5. Passwords must not be included in emails unless they have been encrypted.
6. Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
7. System level and administrative passwords will be kept in a secured manner.
8. Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted of at least once per each calendar quarter.

C. Security Against Outside Influences

1. The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited and violators may be subject to dismissal and prosecution. This portion of the policy does not apply to University technology students who are working in a separate controlled environment.
2. All servers and workstations that connect to the network or cloud systems and that are vulnerable to a virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.
3. Headers of all incoming data including electronic mail must be scanned for viruses by the email server or provider where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
4. Where feasible, system or network administrators should inform users when a virus has been detected.
5. Virus scanning logs must be maintained whenever email is centrally scanned for viruses.
6. Intruder detection must be implemented on all servers and workstations containing data classified as high risk.