

## University Policy

**Policy Title:** Electronic Data and Information System Security

**Policy No.:** 4200.01

**Department:** IT

**Prepared by:** IT

**Approved by:** President

**Effective Date:** 10/08/2009

**Policy Statement:** All City University of Seattle (CityU) information security policies, standards, guidelines and practices shall be coordinated through the Office of the Chief Financial Officer (CFO) and shall be consistent with a university-wide approach in developing, implementing and managing information systems security.

University faculty, staff, students, volunteers, or vendors who have access to CityU 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:

- 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 CityU operations that may be of a sensitive nature

City University of Seattle follows all government regulations (FERPA, etc.) in protecting the privacy of students, faculty and staff information.

**Scope:** 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, internal memos, etc. This policy applies to all information residing on university servers, desktops, laptops, and storage devices.

### Roles and Responsibilities

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

1. **Information Security Officer:** This person is responsible for monitoring compliance with the University Security Policies. The information security officer is the director of information technology, or other designee of the CFO.
2. **Stewards:** Stewards are those members of the CityU community who have responsibility for particular university generated or maintained information and therefore, are responsible for the integrity of that data (e.g., 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 CityU 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, 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 CityU 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 CityU policies and procedures in this regard, and immediately reporting breaches of this policy to the office of the CFO.

### **Data Types**

There are two main kinds of data:

- 1) University-owned data that relates to such areas as financials, employment records, payroll, [etc.]
- 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, contact information, [etc.]

### **Data Classifications**

CityU's data is comprised of two (2) classifications of information:

1. Public/Unclassified information is defined as 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 directory information. Annual reports, tax returns, and audited financial statements are also available as public information but must be coordinated with the Office of the CFO.

Employees may send or communicate public/unclassified non-financial information to anyone inside or outside of the university.

2. Private/Confidential/Restricted 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 data are social security numbers, tax forms, security procedures, employment data, business strategy information, trademark and patent data and other information as applicable.

All information not otherwise classified as Public/unclassified, will be assumed to be Private/Confidential/Restricted and may not be disclosed.

### **Access Control**

1. Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.
2. Where possible and financially feasible, more than one person must have full rights to any university owned server 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 and servers and systems should be achieved by individual and unique logins, and should require authentication.
4. Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents.. All users must secure their username or account, password, and system access from unauthorized use.
5. Passwords must not be placed 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.

### **Virus Prevention**

1. The willful introduction of computer viruses or disruptive/destructive programs into the University production environment is prohibited, and violators may be subject to prosecution. This portion of the policy does not apply to our technology students who are working in a separate, controlled environment.
2. All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that it 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 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.

### **Intrusion Detection**

1. Intruder detection must be implemented on all servers and workstations containing data classified as high risk.

2. Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
3. Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.

**Internet Security**

1. All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk.
2. All connections to the Internet should go through a properly secured connection point to ensure the network is protected when the data is classified confidential.
3. Firewalls and DMZ's will be used to restrict traffic and separate student use networks from faculty/staff production networks.


**System Security**

1. All systems connected to the Internet should have a vendor supported version of the operating system installed.
2. All systems connected to the Internet must be current with security patches.
3. System integrity checks of host and server systems housing high risk University data should be performed.

**Equipment/Data Disposal**

1. All systems that are disposed of will have their hard drives made unusable before disposal.

Revision History			
Review date:	Revised by:	Approval date:	Next review date:
10/2009	IT	10/8/2009	7/1/2011
5/2013	IT	TBD	TBD
Comments:			

  
Unit Head Signature

5/20/13  
Date

A handwritten signature in black ink, appearing to read "Eric Gorch". The signature is written in a cursive style with a large initial "E".

---

President's Signature

Date