Responsible Access and Use of Information Technology Resources and Services Policy

**Functional Area:** Information Technology Services (IT Services)  
**Date Issued:** January 20, 2014

**Applies To:** All users and service providers of Armstrong’s Information Technology resources and services  
**Date of last review:** January 20, 2014

**Policy Reference(s):**  
Data Classification Policy  
USG Information Technology Handbook  
**Date of next review:** July 1, 2014  
**Page(s):** 7

**Responsible Person**

This policy will be re-evaluated on or about the first day of July each calendar year to determine whether all aspects of the policy are up to date and applicable in the current business environments, and will be revised as necessary. The Chief Information Officer is responsible for the review and accuracy of this policy.

**Purpose / Rationale**

This policy sets forth standards for responsible use of Armstrong’s information technology (IT) resources.

**Definitions**

Information technology (IT) resources – Resources which include, but are not limited to computer systems, computer labs, applications, networks, software, VOIP telephones, and data owned, managed, or maintained by the University.

**Policy**

IT resources are the property of the University and shall be designated for University instructional, research, public service, administrative, and approved contract purposes.
Each person with access to Armstrong’s IT resources is responsible for ensuring these resources are used appropriately and for complying with all applicable policies and regulations within the University and with all applicable State and Federal laws and regulations.

All personally owned devices used to store, process, or transmit university information or that are otherwise connected to University IT resources are covered by the policy.

4. Limit the personal use of University Computing Resources and refrain from using those resources for personal commercial purposes or for personal financial or other gain. Personal use of University Computing Resources is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user’s job or other University responsibilities, and is otherwise in compliance with this and other University policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

General Responsibilities for Users of Campus Resources:

- Protect user ID, password, and system from unauthorized use.
- Respect the intellectual property rights of authors, contributors, and publishers in all media.
- Adhere to the terms of software licenses and other contracts.

Prohibited Use of Campus Resources:

- Accessing or attempting to access another's accounts, data, private files, e-mail messages without the owner's permission.
- Exposing sensitive or confidential information or disclosing any electronic information that one does not have the authority to disclose.
- Misrepresenting oneself or affiliation to gain access to IT resources and services.
- Users may not in any way divulge copy, release, sell, loan, alter or destroy any information except as appropriate and required within the scope of their academic or professional duties.
- Altering system software or hardware configurations without authorization; disrupting or interfering with the delivery or administration of IT resources; facilitating access to University IT resources by unauthorized users.
- Engaging in any activity that interferes with the proper functioning of the University’s information technology resources. Examples include, but are not limited to, propagating viruses, damaging files, making unauthorized modifications to University data.
- Violating copyright, University trademark, and/or software agreements or applicable federal and state law by installing, copying, distributing, or using software, music, text, images, and video.
- Using University IT resources for personal gain (i.e. commercial or profit-making purposes)
- Knowingly using IT resources for illegal activities. Criminal or illegal use may include obscenity, child pornography, threats, harassment, defamation, and theft.
Requirements for any computer or mobile device used to access University resources and services

In order to adequately protect University information systems from being compromised, users should conduct university business with security industry-sanctioned best practices that include but are not limited to the following:

- Establish strong passwords for all computer accounts (see Password Requirements below)
- Ensure that passcode or screen locks are enabled on mobile devices
- Lock or log off their computers before leaving them unattended
- Ensure that system and application security updates are applied as soon after being released by the vendor as possible
- Ensure that anti-virus software is installed and is actively protecting the system
- Ensure that all programs, browsers, and service packs are up to date, especially regarding any security releases for those products

Password Requirements

To ensure university information is adequately protected, the following composition rules need to be followed when passwords are created for computer accounts and resource access (e.g., Gmail, Port):

- Passwords need to be at least eight characters in length.
- Passwords need to include at least one character from each of the following character groups:
  - upper case alphabetic characters (A-Z)
  - lower case alphabetic characters (a-z)
  - numbers (0-9)

All passwords should be periodically changed to protect the integrity of the authorization process to University resources.

Passwords must never be shared or stored in a location accessible by others. If a user suspects passwords may have been compromised, it is the user’s responsibility to contact IT Services for procedures related to password resets. If the resource used is not under the control or operation of IT Services, but another approved agency, then the user is responsible for contacting the appropriate party for assistance.

Passwords used to access confidential information should be unique from personal passwords used outside of University responsibilities.

The University's right to access files

Subject to applicable law, the University reserves the right to access and copy files and documents (including e-mail and voicemail) residing on University-owned equipment. The University may be required to produce data in compliance with a valid subpoena or court order.
Non-intrusive monitoring of campus network traffic occurs routinely, to assure acceptable performance and to identify and resolve problems. If problem traffic patterns suggest that system or network security, integrity, or performance has been compromised, network systems staff will investigate and protective restrictions may be applied until the condition has been rectified.

**Ensuring network performance**

Users must not attempt to intercept, capture, alter, or interfere in any way with information on local, campus or global network pathways. This also means users may not run "sniffers" (programs used to capture information being transmitted) on the campus network or any portion thereof without authorization from CIO or designee. Users may not operate Dynamic Host Configuration Protocol (DHCP) servers on the campus networks.

Users must not attempt to obtain system privileges to which they are not entitled, whether on University computers or on systems outside the University. Attempts to do so will be considered serious offenses which may result in a denial of access to University information technology resources, and other appropriate disciplinary actions.

Computer procedures, programs and scripts that permit unauthenticated or unauthorized senders to send e-mail to arbitrary recipients from unrestricted sources are prohibited.

Users must refrain from creating and/or implementing code intended to periodically or randomly interrupt computer systems or services. Users must not intentionally propagate computer viruses.

Users must not conduct unauthorized port scans. Users must not initiate nuisance or denial-of-service attacks, nor respond to these in kind. Malicious use of any device or method to disrupt network services or lessen the integrity of system data will be considered a serious violation of University regulations.

Wireless access points may not be installed without authorization from IT Services in campus academic, administrative, or service buildings, including buildings rented or owned by the University off-campus.

Respect the finite capacity of University Computing Resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of University Computing Resources, the University may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

**Managing and protecting confidential information**

Employees are prohibited from accessing information that has been classified as confidential to include Personally Identifiable Information (reference Data Classification Policy for definitions) unless such access is related to the employee's duties and approved by his/her supervisor. For information classified as confidential, such authorization may be granted to a specific individual or to all individuals serving in a specific job function. For university employees, access to confidential data is determined by business process. For non-university employees, access shall be determined by the appropriate manager in conjunction with the General Counsel’s office.
For information classified as confidential, the following procedural and system-level controls must be in place:

- Departmental procedures must be in place to ensure that all individuals are aware of the sensitivity of the information to which they have access and understand their responsibilities to protect that information appropriately.
- Tangible records (e.g., memos, reports, paper documents) containing confidential information must be stored in a locked cabinet or drawer when not in use. Documents must be physically shredded/destroyed when no longer needed.
- Procedures must be in place to control physical access to electronic devices that store confidential data.

Employees who store or transmit information classified as confidential should encrypt both the stored data and its transmission.

As a general rule, confidential data should not be stored on laptop computers, flash drives, smart phones, or other devices that are easy to carry away. If it is absolutely necessary to store sensitive or confidential information on such a device, the information should be encrypted to protect it from view should the device fall into unauthorized hands.

Employees who store or transmit confidential data on portable devices are responsible for ensuring that the information is backed up regularly in a form that permits ready retrieval.

In the event of unauthorized access to University data, whether through theft or loss of portable devices such as USB drives, laptops, smart phones or other devices, or any other kind of breach of security, the individual who is responsible for the device or who learns of a potential breach must notify the ISO and assist with the University’s data breach response. In case of theft of University-owned equipment, this individual must also contact University Police.

The University-endorsed encryption product or protocol should be used whenever possible. Employees should consult IT Services for an appropriate product or protocol.

**Data Security Practices and Requirements**

**All Employees:**

1. Must ascertain and understand the classification level of information (reference Data Classification Policy) for which they have been authorized to access.
2. Must adhere to University’s requirements for protecting any computer used to conduct University business regardless of the sensitivity level of the information held on that system (see Requirements for any computer used to conduct University business section below).
3. Must protect the confidentiality, integrity and availability of the University's information as appropriate for the information's sensitivity level wherever the information is located (e.g., physical documents, storage media, telecom system or data networks).
4. Must safeguard any physical key, ID card or computer/network accounts that allow them to access University information. This includes creating difficult-to-guess computer passwords (see Password section below).
5. Must destroy or render unusable any confidential information contained in any physical document or any electronic, magnetic or optical storage medium (e.g., USB drive, CD, hard disk, magnetic tape, or diskette) before it is discarded.

6. Must report any activities that they suspect may compromise sensitive information to their supervisor and the University Information Security Officer.

7. Must protect sensitive information even after leaving the University.

8. Must consult General Counsel upon receiving investigative subpoenas, court orders, or any other requests for confidential information.

Additional Responsibilities for Supervisors and Managers:

In addition to complying with the requirements listed above for all University employees, managers and supervisors should:

1. Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the Information Security Officer (ISO) or appointee, and that those procedures are followed.

2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.

3. Ensure that each employee understands his or her information security-related responsibilities.

4. Ensure that the requirements for confidentiality, integrity and availability are satisfied within their environments by:
   - Developing, implementing, operating and maintaining a secure technology environment that includes:
     - A comprehensive document relating to the design and access management of services and systems
     - Product implementation and configuration standards
     - Procedures and guidelines for administering network and system accounts and access privileges in a manner that achieves the appropriate level of data security and allows employees to perform their required job functions
     - An effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted best practices for the technology
   - Ensuring that employees are trained on proper procedures for the classification and handling of data and the measures used to secure it.

5. Departments that maintain servers or internal networks are expected to protect the privacy of those using the resources and are responsible for managing access.

Additional Responsibilities for Information Technology Services Employees:

IT Services maintains and operates both internal and external resources that house, transmit, and create user information and data. As such, IT Services has developed appropriate safeguards and security related procedures.

IT Services will perform periodic review of these internal and external resources. These reviews will
include, but are not limited to, the following:

- Appropriate administrator access level for each IT Services staff position
- Firewall configuration review of systems and network resources
- Log reviews
- Service patches, anti-virus, malware protection review
- System load and performance review
- Disaster recovery procedures review
- Backup status/location
- Verification of backups

Nothing in this policy should be construed to supplant the special jurisdictions and procedures set forth by federal or state laws or USG policies.