



Creighton University

Information Security Philosophy

Revision (pre-release draft): 7
File Name: SEC_PHILV6
Last Save Date: 11/4/2002 3:55 PM

TABLE OF CONTENTS

1. PURPOSE	1
2. SCOPE.....	1
3. INFORMATION SECURITY.....	1
4. COMPLIANCE REQUIREMENTS.....	2
5. DEFENSE IN DEPTH	2
6. ROLES AND RESPONSIBILITIES	2
7. SECURITY ADMINISTRATION	4
7.1 INFORMATION CLASSIFICATION.....	4
7.2 SECURITY AWARENESS	5
7.3 SECURITY VIOLATIONS AND SANCTIONS	5
7.4 COMPUTER CRIME.....	5
7.5 ACCESS MANAGEMENT	6
7.6 MANAGED SERVICES.....	6
7.7 INCIDENT RESPONSE	6
7.8 ENCRYPTION.....	6
7.9 EXCEPTIONS TO POLICIES AND STANDARDS	7
8. APPROPRIATE USE OF INFORMATION ASSETS	7
8.1 GENERAL USE OF COMPUTING AND NETWORK RESOURCES.....	7
8.2 AUTHORIZED USAGE	7
9. INFORMATION ACCESS CONTROL	8
9.1 PHYSICAL ACCESS	8
9.2 MEDIA AND HARDCOPY PROTECTION.....	8
9.3 LOGICAL ACCESS CONTROLS	8
9.4 TERMINATION OF ACCESS	9
9.5 PROTECTION OF PRIVATE INFORMATION	9
9.6 SECURITY LOGGING	9
10. DATA COMMUNICATIONS SECURITY	9
10.1 COMMUNICATIONS SECURITY.....	10
10.2 RELEASE OF PATIENT IDENTIFIABLE INFORMATION.....	10
10.3 ELECTRONIC COMMUNICATIONS AND CREIGHTON COMPUTERS.....	10
10.4 INTERNET USAGE	10
10.5 REMOTE ACCESS.....	11
10.6 WIRELESS SECURITY	11
10.7 FIREWALL.....	11
11. INFORMATION INTEGRITY CONTROLS	12
11.1 ANTI-VIRUS CONTROLS	12
11.2 APPLICATION DEVELOPMENT AND ACQUISITION CONTROLS	12
12. PREVENTATIVE CONTROLS	12
12.1 BACKUP AND RECOVERY	12
12.2 CONTINGENCY PLANNING	13

1. PURPOSE

This document communicates Creighton University's philosophy towards Information Security. The objectives of this document are to communicate the steps taken to:

- i. Protect the University's mission by taking the necessary steps to protect information in all forms.
- ii. Prevent loss or misuse of information, which is considered an asset of Creighton University.
- iii. Protect information from accidental or intentional destruction, disclosure or modification throughout its life cycle.
- iv. Ensure compliance with applicable regulations and the privacy policies of Creighton University with respect to staff, faculty, students, patients, customers and business partners.
- v. Establish responsibility for access and use of Creighton University information assets and resources.
- vi. Establish a basis for compliance, risk management and audit of information security.

2. SCOPE

This document applies to the entire Creighton University community. It is Creighton University's intent that this document be fully implemented and followed.

Creighton University's information assets include data, image, text, and voice assets within internal systems, as well as, Creighton University and/or vendor supplied information processing equipment, terminals, small systems (e.g. personal computers), supporting facilities and information processing services.

3. INFORMATION SECURITY

Information and information systems are critical Creighton University assets. Without reliable and properly secured information and information systems, Creighton University is open to unnecessary liabilities. Likewise, the preservation and enhancement of the University's reputation is directly linked to the way in which both information and information systems are managed. Maintaining an adequate level of security is one of several important aspects of both information management and information systems management.

To be effective, information security must involve the participation and support of the entire Creighton University community. In recognition of this need for teamwork, this security document clarifies the responsibilities of users as well as the steps they must take to help protect Creighton University information and information systems.

Guidance, direction, and authority for information security activities are centralized for the entire University in Information Technology under the Information Security Officer.

4. COMPLIANCE REQUIREMENTS

University departments, divisions, or schools may write specific policies and standards as long as these policies and standards do not detract from the University's Information Security Philosophy, Policies, or Standards.

5. DEFENSE IN DEPTH

A primary Information Security objective is to protect the information resources through Defense in Depth. The underlying principle to Defense in Depth is implementing layers of security to protect information assets. A Defense in Depth strategy combines the abilities of people, technology, and operations to establish multiple layers of protection. The objective of Defense in Depth is to implement security mechanisms at multiple locations so critical resources are protected and can continue to operate in the event that one or more of the mechanisms are circumvented. The layers of defense employed to secure the university's assets include: security policies, employee awareness, firewalls, intrusion detections systems, security logging and monitoring, strong passwords, cryptography, anti-virus, and physical security. None of these defenses alone provide adequate protection, however, when layered these mechanism can provide a strong security infrastructure.

6. ROLES AND RESPONSIBILITIES

Information Security Officer: The information security officer is responsible for implementing and monitoring a consistent information security program. The Information Security Steering Committee will monitor this responsibility. The information security officer will:

- i. Coordinate the development and maintenance of information security policies and standards.
- ii. Coordinate information security activities with all university entities.
- iii. Monitor security activities and oversee the application of specific security policies.
- iv. Implement and maintain the security infrastructure.
- v. Assist information custodians and systems administrators in assessing their data for classification and advise them of available controls.
- vi. Implement and maintain an information security awareness program.
- vii. Provide consulting services for information security throughout the university.

Information Security Steering Committee: The information security steering committee is comprised of representatives from across the university and acts as a council for information security for the entire university.

Internal Audit: The internal audit department proactively reviews systems and services for compliance with information security standards and policies, other internal standards, and the requirements of external regulatory bodies.

To coordinate the team effort referred to in the Information Security document above, Creighton University has established three categories, at least one of which applies to each member of the Creighton Community. These categories are Custodian, Systems Administrators, and User. These categories define general responsibilities with respect to information security.

Information Custodians: Custodians are the Department Heads, Managers, or their delegates within Creighton University who bear responsibility for a particular set of information. Information custodians are responsible for implementing information security policies and standards concerning their information. Information custodians will:

- i. Assume responsibility for the information.
- ii. Recommend appropriate business use of the information.
- iii. Authorize information access.
- iv. Communicate control and protection requirements to systems administrators and users.
- v. Monitor compliance and periodically review requirements of information protection.

Systems Administrators: Systems Administrators are in physical or logical possession of either Creighton University information or information that has been entrusted to Creighton University. While Information Technology staff members clearly are systems administrators, local IT groups are also systems administrators. Whenever information is maintained only on a personal computer, the User is also the systems administrator. Each type of information must have one or more designated systems administrators. Systems Administrators will:

- i. Administer custodian-specified business and information protection controls.
- ii. Administer access control.
- iii. Provide backup and recover of information.
- iv. Detect and respond to violations and weaknesses.
- v. Monitor compliance with information security policies and standards.

Information User: Users of Creighton University information will:

- i. Familiarize themselves with and comply with all information security policies and standards
- ii. Access only the information for which they are authorized.
- iii. Maintain information, in their possession, in accordance to the custodian's recommendations.
- iv. Report suspected or actual violations of policies and standards.
- v. Report suspected or actual security breaches or compromises.

7. SECURITY ADMINISTRATION

It is the responsibility of the Information Security Officer to develop and maintain the Information Security program within Creighton. The Information Security program provides policies and standards for administering the protection of Creighton's information assets.

7.1 INFORMATION CLASSIFICATION

Creighton University has adopted an information classification system that categorizes information into three groupings. All information under Creighton University's control, whether generated internally or externally, falls into one of these categories: PUBLIC, INTERNAL, or CONFIDENTIAL. It is the information custodian's responsibility to assess risks and threats to information under their purview and classify their information accordingly. Every member of the Creighton community is expected to familiarize themselves with the definitions for these categories and the steps that must be taken to protect the information falling into each of these categories. Recommendations for handling information are outlined in the table below:

	PUBLIC	INTERNAL	CONFIDENTIAL
Label	None	None	Marked "CONFIDENTIAL"
Access	Minimal controls to prevent unauthorized modifications.	Access controls appropriate to the value of the information	Limited based on 'need to know'.
Storage	Minimal controls to prevent unauthorized modifications.	Store out of sight of non-Creighton persons	Lock up
Communication	Minimal controls to prevent unauthorized modifications.	Minimal controls to prevent unauthorized modifications.	Confidential envelope; Secure transmission
Destruction	No Controls	Shred paper	Shred paper; Overwrite media

Further details can be found in the [Information Classification Policy](#).

7.2 SECURITY AWARENESS

Within the University, people represent both the greatest assets and greatest threats to information security. The most probable form of information compromise is through inadvertent or careless disclosure by authorized users. Employee awareness can substantially minimize the risk of information loss. All information users should receive regular security awareness training.

For additional information, see the [Security Awareness Training Policy](#).

7.3 SECURITY VIOLATIONS AND SANCTIONS

Information resources are valuable assets strategically provided to further business, research, administrative, and academic functions of Creighton University. Individuals using information resources owned or managed by the University are expected to know and comply with applicable Creighton University policies, standards, and local, state and federal laws. Individuals are responsible for the security of any computer account issued to them and will be accountable for any unauthorized activity that takes place with their account.

7.4 COMPUTER CRIME

Members of the Creighton University community are encouraged to utilize the resources that are available on the University network and the Internet. Users should note that federal and state laws as well as Creighton University policies also govern their usage. Violation of State and Federal laws or Creighton University security policies may result in immediate suspension of access privileges or other disciplinary action as appropriate to the situation.

Computer Crime violates state and federal laws. Computer crime includes, but is not limited to:

- unauthorized disclosure, modification, or destruction of data, programs, or hardware
- denial of computer services
- theft of computer services
- illegal copying of software
- invasion of privacy
- theft of hardware, software, peripherals, data, or printouts
- misuse of communication networks
- promulgation of malicious software such as viruses
- breach of contract

Violators can be prosecuted under state and federal laws, held civilly liable for their actions, or both.

7.5 ACCESS MANAGEMENT

The act of granting secure access to computer-based applications is critically important to maintaining a secure IT environment.

Access will be granted on a need to know basis. Access will be granted only after proper, documented, approval has been obtained. All information users will be assigned unique credentials that will be used to access the authorized resources.

For additional information, see the [Access Control Policy](#).

7.6 MANAGED SERVICES

When subject matter expertise is not available in house, it makes sense to seek that expertise from outside vendors. Many outside vendors offer managed services. These arrangements offload the burden of highly complex or redundant operations to organizations that specialize in the particular field. When you offload computer functions to outside organizations you introduce new vulnerabilities.

Contracts for system and/or application management must include security, confidentiality, non-disclosure, and audit clauses. These clauses must specify adherence to Creighton's information security policies and standards.

7.7 INCIDENT RESPONSE

A strong security program will reduce the risks to confidentiality, integrity, and availability of data; but it will never fully eliminate the risk. Since some level of risk will always be present, it is only prudent to be prepared to address any incident.

If a security breach is suspected, the Information Security Officer should be notified immediately. The Incident Response Plan will be followed for all suspected and actual security breaches.

For additional information, see the [Incident Response Policy](#).

7.8 ENCRYPTION

Information may be in one of three states while being maintained by Creighton. The states are information in storage, information being processed, and information in transit. Security of information is critical to Creighton's missions. The best and most secure means of protecting information in storage and in transit is the use of encryption. Encryption is the process of mathematically changing readable text into non-readable

text. Encryption is a mechanism that will add an addition layer of protection under the principle of Defense in Depth.

All methods of encryption must be approved by Information Technology.

For additional information, see the [Encryption Policy](#).

7.9 EXCEPTIONS TO POLICIES AND STANDARDS

Policies and Standards are management instructions indicating a course of action. Compliance with policies and standards are mandatory.

All exceptions to the Security Policies and Standards are to be requested in writing and approved by the Information Security Steering Committee.

For more information on the exception process see the [Information Security Exception Policy](#).

8. APPROPRATE USE OF INFORMATION ASSETS

Access to Creighton's information resources is provided to users for a wide variety of purposes. It is important that Creighton University users be aware of their individual obligations and what constitutes proper use and behavior.

8.1 GENERAL USE OF COMPUTING AND NETWORK RESOURCES

Creighton provides computing resources to facilitate University business. Users should utilize resources in a manner that is consistent with the mission of Creighton University. Appropriate use and behavior demonstrates a respect for:

- The rights of others to privacy;
- Intellectual property rights (e.g., licenses and copyrights);
- Ownership and custodianship of data and information resources;
- System mechanisms designed to limit access;
- The ethical use of University-owned resources; and
- The right of individuals to be free of intimidation, harassment, and unwarranted annoyance.

Any action or misuse of information resources that harms the resources of Creighton or adversely affects other users is prohibited.

8.2 AUTHORIZED USAGE

Standards are established for ethical use of information to protect the interests of patients and other constituents and to prevent misuse of information vital to Creighton University.

Unauthorized uses of Creighton computing resources would include, but are not limited to, such activities as:

- Users may not attempt to gain access to computer systems to which they are not authorized.
- Users may not deliberately attempt to disrupt the performance of a computer system or a network.
- Users may not attempt to break system security.
- Users may not read, execute, or access a file owned by another user unless granted permission.
- Users may not seek to determine another person's password, through cracking, decryption, interception or other means.
- Users may not use the network in any way to harass another user of the network.

For more information, see the [Responsible Computing Handbook](#).

9. INFORMATION ACCESS CONTROL

Access controls are employed to protect information and must be applied to information on all platforms and media. The level of control used is dictated by the value of the information to Creighton University and its customer/patients.

9.1 PHYSICAL ACCESS

The first step in securing information and information resources is to restrict physical access to the information or information resources.

Creighton's computer systems, which store protected health information or other CONFIDENTIAL information, must adhere to stringent physical controls.

For additional information, see the [Physical Access Policy](#).

9.2 MEDIA AND HARDCOPY PROTECTION

Electronic media and hardcopies of sensitive information must be protected during transportation, storage, processing and destruction.

For more information, see the [Media Control Policy](#).

9.3 LOGICAL ACCESS CONTROLS

Access controls are employed to protect information and must be applied to information on all platforms and media. The level of control used is dictated by the value of the information to Creighton University and its customers/patients.

A written request must be made to obtain system privileges. Access to information will be granted based on least privilege or “need-to-know.”

For more information see the [Access Control Policy](#).

9.4 TERMINATION OF ACCESS

Access to University systems should be granted on a “need-to-know” basis. Termination of access will occur when a user no longer has a need for the specific access.

For more information, see the [Termination of Access Policy](#).

9.5 PROTECTION OF PRIVATE INFORMATION

In the course of its business, it is necessary for Creighton University to record, store, process, transmit, and otherwise handle private information about individuals. Creighton takes these activities seriously and seeks to provide fair, secure and legal systems for the appropriate handling of this private information. All such activities at Creighton University are additionally intended to be consistent with generally accepted privacy, ethics, and standard business practices.

Private information maintained by Creighton University shall be secure from accidental or inappropriate disclosure. Private information shall be used only as intended, and precautions preventing misuse must be taken.

For more information see the [Data Classification Policy](#).

9.6 SECURITY LOGGING

Even the best security is not going to guarantee that data is never unintentionally changed. To lessen risks associated with granting access to data, security logging shall be employed where feasible and appropriate. Security logging will not prevent changes to data, but it will provide an audit trail used to detect when information was accessed, changed, or deleted.

For more information, see the [Audit Trail Policy](#).

10. DATA COMMUNICATIONS SECURITY

All information traveling over Creighton University’s computer networks that has not been specifically identified as the property of other parties will be treated as though it is a

Creighton University asset. It is the policy of Creighton University to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

10.1 COMMUNICATIONS SECURITY

Information transmitted outside the organization requires protection. Methods employed will depend upon information sensitivity, technical risks and threats, external regulations and available communication security controls. All data communications networks will have appropriate logical and physical controls to restrict access to authorized users.

10.2 RELEASE OF PATIENT IDENTIFIABLE INFORMATION

The privacy/security provisions of the federal law; HIPAA and FERPA, state that the privacy and security of patient health and student personal information must be protected.

Release of patient health and student personal information will occur only in accordance with federal law and Information Security Policies and Standards. The policies and standards cited in Creighton's Information Security documents will apply to all entities and subdivisions.

10.3 ELECTRONIC COMMUNICATIONS AND CREIGHTON COMPUTERS

Members of the Creighton community are encouraged to use electronic mail, voice-mail, and university computers for university-related activities and to facilitate the efficient exchange of useful information. Access to electronic mail, voice-mail, and university computers is a privilege and certain responsibilities accompany that privilege.

By using Creighton University's electronic mail and voice-mail systems and the utilization of other communications equipment (including Creighton computers), users knowingly and voluntarily consent to being monitored by Creighton University, acknowledging Creighton University's right to conduct such monitoring, and acknowledge that they have no expectation that said systems, communications, and equipment are private to any employee.

Electronic and telephone communications, including electronic mail and voice-mail communications, mailboxes and systems, and the contents of computers provided by Creighton are the sole property of Creighton University.

For more information see the [Electronic Communications Policy](#).

10.4 INTERNET USAGE

Creighton University's computer network is connected to the Internet. Everyone with access to Creighton's network has the ability to access the Internet. While the Internet is

a great resource for the University, it is the responsibility of each user to use this resource responsibly and respectfully.

All use of the Internet via Creighton University resources must be in compliance with all applicable laws and University policies. Internet access via Creighton University resources, therefore, must not be used for illegal purposes.

The safety and security of Creighton University's network and resources must be considered at all times when using the Internet. Internet users are responsible for adhering to applicable Creighton University policies and standards.

Network services available via the Creighton network will be limited to those required for Creighton business.

Each individual user is responsible for complying with this and all other relevant policies when using Creighton University resources for access to the Internet.

For more information, see the [Acceptable Use Policy](#).

10.5 REMOTE ACCESS

Remote access to university systems is a productivity and creativity enhancer; however it also introduces new vulnerabilities for Creighton University. It is critical to the integrity of Creighton's information systems that all remote access adheres to the Remote Access Policy rules regarding password transmission, connections to outside systems, and connections to public access networks.

For more information, see the [Remote Access Policy](#).

10.6 WIRELESS SECURITY

Due to the risks inherent in wireless networking all implementations of wireless networking must comply with all Creighton policies and standards.

For more information, see the [Wireless Networking Policy](#).

10.7 FIREWALL

The first layer of defense in the Defense in Depth principle is to protect the network's entry points. To provide security while allowing access to information, a secure network infrastructure must be in place. The infrastructure must include a network segment for all public access systems, and a secure internal network for critical backend systems. Information must flow between the public and secure network freely, but securely. The security for these network segments is provided, in part, by firewalls. Firewalls are hardware or software based devices designed to prevent unauthorized access to or from a

private network. Firewalls use rules to define the types of network traffic that is allowed to pass. It is critical to network security that firewall rules function as intended.

For more information, see the [Firewall Policy](#).

11. INFORMATION INTEGRITY CONTROLS

11.1 ANTI-VIRUS CONTROLS

Personal computers and local area networks are susceptible to becoming infected by viruses that can cause system malfunction and data loss. A virus should never be assumed harmless and left on a system. Network users are responsible for ensuring they have the most current version of Virus Protection Software loaded on their workstation. The Help Desk can help identify and replace old version of the software.

For more information, see the [Virus Prevention Policy](#).

11.2 APPLICATION DEVELOPMENT AND ACQUISITION CONTROLS

The stability of Creighton's computing resources are critical to efficient operation. To ensure stability, among other thing, changes to any centrally managed system must be controlled. All computer and communications systems used for mission critical applications at Creighton University will employ a documented change control process, which is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures. Again, this policy applies to personal computers running production systems, just as it applies to larger multi-user systems.

All production software development and software maintenance activities performed by in-house staff must subscribe to Information Security policies, standards, guidelines, and other systems development conventions. Among other things, these conventions include the proper testing, training, and documentation.

For more information, see the [Configuration Management Policy](#).

12. PREVENTATIVE CONTROLS

12.1 BACKUP AND RECOVERY

To protect Creighton University's information resources from loss or damage, personal computer users are responsible for regularly backing-up the information on their personal computers, or else making sure that someone else is doing this for them. For multi-user computer and communication systems, a Systems Administrator is responsible for making periodic back-ups. All back-ups containing critical and/or sensitive information must be stored at an approved off-site location with physical access controls or

encryption. A contingency plan must be prepared for all applications that handle critical production information; it is the responsibility of the information custodian to make sure that this plan is adequately developed, regularly updated, and periodically tested.

For more information, see the [Contingency Planning Policy](#).

12.2 CONTINGENCY PLANNING

The survival of Creighton University in today's environment is dependant on the continuity and safeguarding of Creighton's information assets, adequate staffing, efficient communications, and computing resources. Interruption or impairment of these elements would have a devastating effect on Creighton's ability to meet its mission. A lengthy interruption would have disastrous impact on Creighton's ability to conduct business. Contingency planning outlines the process of establishing strategies to minimize the effects of a disruption and ensure timely resumption of operations. Backup and archival strategies focus on recovery from short-term and equipment failures, whereas contingency planning describes a more structured process of planning for long-term outages and disasters. Creighton will maintain a current and tested contingency plan.

For more information, see the [Contingency Planning Policy](#).