	Wright State University Information Security	

Controls	
Policy Title:	Information Security Framework
Category:	Information Technology
Audience:	WSU Faculty and Staff
Reason for Revision:	*N/A*
Created / Modified Date:	7-1-09
Next Review Date:	7-1-11
Location:	http://www.wright.edu/security/policy/

Responsible Parties	
Author	Michael Natale
Technical Reviewer/Mgr	Michael Natale
Security Reviewer	Michael Natale

TABLE OF CONTENTS

DESCRIPTION & PURPOSE **4**

POLICY STATEMENT **4-5**

INFORMATION SECURITY PROGRAM **5-9**

ASSOCIATED POLICIES **10**

Wright State University Information Security Framework

The Department of Information Security recognizes that information assets generated, collected, used, and maintained by the University in course of conducting everyday activities are subject to varying degrees of concern with respect to security and privacy. The Storage of university data on computers and the transfer of that data across the network ease use and expand our functionality. Commensurate with that expansion is the need for the appropriate security measures. This policy endeavours to balance the need for effective information security practices, with the usability of the systems and business processes in place at the University.

Each department within the University should apply this policy to meet their information security needs. In some cases the technology installed may limit immediate compliance with the Policy. Instances of non-compliance must be reviewed and approved by the information security function.

The principles of academic freedom and free exchange of ideas apply to this policy, and this policy is not intended to limit or restrict those principles.

Purpose

This policy outlines the information security program within Wright State University. Wright State's financial, administrative, and student systems are accessible via the campus network and in some cases via the internet. Due to this accessibility these systems are potentially vulnerable to security breaches which could expose the University to the compromise of sensitive data, asset loss, and other risks.

An information security program is necessary to ensure that the University establishes a university-wide approach to information security. This university-wide approach will assist the University in complying with federal and state statutes and regulations regarding the collection, maintenance, use, and security of information assets. To accomplish compliance with this policy it is essential that reasonable and effective practices for the protection and security of information assets be established and implemented; including the protection of sensitive and confidential information against accidental or deliberate unauthorized disclosure, modification, or destruction.

The intent of this policy is to ensure the University meets or exceeds its legal and ethical responsibilities for securing its critical and sensitive information assets.

Policy Statement

It is the policy of Wright State University to utilize effective information security practices that are generally accepted within the higher education community as meeting due diligence requirements.

The University prohibits the unauthorized use, access to, tampering with, alteration of, intentional destruction of, or loss of Wright State's information assets.

The University recognizes that no single office, policy, or procedure provides absolute security, therefore, all University employees and other stakeholders share responsibility to minimize risks and to secure the information assets within their control.

The information security department, overseen by the CIO of Computing and Telecommunications Services and guided by the CISO, has been established within the University. Individuals within the information security organizational structure of the program are empowered to research, develop, implement, and disseminate operational policies, procedures, standards, guidelines, and other processes to support effective information security practices.

The vice presidents, deans, and directors of each college or department shall be responsible for ensuring appropriate information security controls are practiced within their areas of responsibility. Each shall appoint an individual to partner with the department of Information Security to develop, implement, and maintain workable and effective information security practices.

Campus-wide security awareness, training, and education are vital to information security. Therefore the University will develop and maintain such a program. It is imperative that, each college and department ensure that individuals attend University offered security training.

The Director of Computing and Telecomm Services will review the Information Security Program annually.

Information Security Program

1. Information Security Program Overview

For the purposes of this document, *Institutional Data* is defined as all data created, collected, maintained, recorded, or managed by the university, its staff, and agents working on its behalf. Wright State University acknowledges that *Institutional Data* is subject to varying degrees of risk regarding security and privacy. The University has a responsibility, and in some cases may be required by statutes, to manage and protect *institutional data*. This policy endeavors to balance the need for effective information security practices, with the usability of the systems and business processes in place at the University. To protect *institutional data* and their associated information systems, Wright State University has established an Information Security Program to assist in guiding the University in effective security practices and procedures. The majority of the security measures taken will affect the Information Technology departments who manage and administer information systems; however, it is abundantly clear that a collaborative effort between all stakeholders is required.

2. Program Purpose and Objective

The purpose of the information security program is to ensure the confidentiality, integrity, and availability institutional data and the systems housing this information. This program objectives are: to identify incidents that have resulted or may result in a breach of this information; develop processes to respond to, mitigate damages resulting from, and prevent recurrence of information security incidents; establish a communication process through which each college and department is aware of their responsibilities and are involved in the security process.

3. Information Security Roles and Responsibilities

An Effective information security program requires clear direction and commitment from top management and administration. To be effective, information security must be an integrated function that requires effective direction and collaboration throughout the University. The roles and associated responsibilities must be clearly defined and understood.

Controls and safeguards must be designed and implemented to mitigate the risks identified and assessed. The College must review current safeguards implemented to mitigate identified risks, and recommend/coordinate implementation of additional safeguards as required. Administration and management should regularly review implemented safeguards to control the risks identified through risk assessments and ensure regular tests or other monitoring of the effectiveness of such safeguards is conducted. Primary safeguards include:

1. Employee Training and Management Processes
2. Information/Information Systems Controls
3. System Failure Management
4. Overseeing Service Providers

3.1 Vice-Presidents

Vice-Presidents hold the primary responsibility for information collected, maintained, and/or "owned" by their areas of responsibility. Vice-Presidents may delegate operational management of these responsibilities by designating an individual to act as a *Liaison* to the Information Security Department. Vice Presidents may also designate other responsible individuals to work with the designated *Liaison* to assist in implementing this program. These designated individuals ensure information assets within their span of control are identified, have designated responsible parties or owners, that risk assessments are carried out for departments under their purview, and that mitigation processes based upon those risks take place.

3.2 Deans, Directors, Chairs, Managers, and other Supervisors

Deans, Directors, Chairs, Managers, and other Supervisors responsible for managing employees with access to *Institutional Data* and associated information systems are responsible for specifying, implementing, and enforcing the specific information security controls applicable to their respective areas. This includes ensuring all employees understand their individual responsibilities related to information security; attend information security training offered by the University; employees have the necessary access to perform their duties; access to information does not exceed the required level for each individual assigned duty. Supervisors should perform an annual review of all users' access levels to ensure they are still appropriate, and take appropriate action to correct discrepancies and/or deficiencies. Supervisors must immediately notify Human Resources and the CaTS Help Desk of any change in employment status that impacts access requirements. Supervisors are also responsible for reporting suspected misuse or other information security incidents to the CISO and/or other appropriate party.

3.3 CISO (Chief Information Security Officer)

The CISO is designated as the individual responsible for coordinating and overseeing the Information Security Program. The CISO is required to work closely with the designated liaisons from all Colleges and Departments, assisting them with information security best practices and establishing reasonable security guidelines and measures to protect *Institutional Data* and systems. This position will oversee the monitoring and management of systems security vulnerabilities; conducting and/or coordinating information security audits; and assisting with investigations, resolution of problems, and/or alleged violations of University information security policies. Questions regarding the information security program should be initially directed to the CISO.

3.4 Department of Information Security

The primary mission of the Department of Information Security is to ensure effective security measures are in place to maintain the

confidentiality, integrity, and availability of University *institutional data* and systems. This mission will be accomplished by ensuring security controls are commensurate with the level of risk and the magnitude of harm resulting from any possible loss, misuse, unauthorized access, or modification of institutional data. Primary objectives include development and implementation of proactive measures to prevent security issues, and effective response to security issues if prevention methods prove ineffective.

3.5 Computing and Telecommunications Services

The Department of Computing and Telecommunication Services (CaTS), including Client Services, Information Services, and Technical Services, is primarily responsible for the integration of technical information security tools, controls, and practices in the network environment and application environment, operating system environment, desktop environment, security awareness training, and is the end-users' initial contact point for reporting suspected information security failure or incidents. CaTS staff must develop and follow information security best practices for managing infrastructure and services.

3.5.1 CaTS - Client Services

Client Services staff members are responsible for providing information security training, providing the first line of contact for the majority of security incidents, as well as establishing and maintaining a secure desktop operating system environment. Client Services staff must be knowledgeable of the established information security policies in place.

3.5.2 CaTS - Information Services

Information Services is primarily responsible for practicing, developing, integrating, and implementing industry accepted security best practices for the University's application environment, such as the administrative system and web applications. It is also responsible for advising (web) application developers in the use of industry accepted application security principles, to make existing and new applications more secure.

3.5.3 CaTS - Technical Services

Technical Services staff members are responsible for ensuring established information security policies and best practices are applied to the configuration and management of the server environment, logical network environment and physical network architecture, operations, and telephony system.

3.6 Employees with Access to information

Employees with access to information and information systems must abide by applicable University policies and procedures, as well as any additional practices or procedures established by their College or

Department. Employees must use and safeguard *institutional data* as governed by the regulations and the duties and responsibilities of their position. This responsibility includes protection of their account password; any data files which contain *institutional data* that are utilized in the performance of their assigned duties; and any other protection the account has. This responsibility extends to reporting suspected misuse or information security incidents to the appropriate party (usually their supervisor).

3.7 Temporary staff, consultants, service providers

Temporary staff members (including student workers) are considered employees and have the same responsibilities as regular full- or part-time employees with access to information and information systems. Supervisors of temporary employees have the responsibilities associated with their section. Consultants, service providers, and other contracted third parties will be granted access to information on a 'need to know' basis. If a third party requires an account for information access, a Wright State employee must 'sponsor' the third party by submitting a written request signed by the third party requestor and the sponsor, and approved by the appropriate vice-president, dean, or director. It is the sponsor's responsibility to ensure the third party user understands the individual responsibilities related to the network account. The user is responsible for the security of his/her password(s) and accountable for any activity resulting from the use of his/her user ID(s) within reasonable scope of his/her control. Third party network accounts will be active for a maximum of one year. If account access is no longer required before a year's time has elapsed, it is the sponsor's responsibility to notify CaTS to cancel the network account. If the account is needed for more than one year, it is the sponsor's responsibility to renew the account prior to the expiration date by submitting an updated (written) request. Third parties shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentially, integrity, and availability of all electronically managed information.

3.8 Students, community members

Students and community members are primarily responsible for the integrity of their own information and for reporting discrepancies to the appropriate office. Students and community members who are granted user accounts must comply with the University's Acceptable Use Policy. This includes being responsible for all activity conducted via their University user accounts, including protection of their passwords and any other protection the accounts have, as well as reporting suspected misuse or information security incidents.

Associated WSU Policies

Policy for Responsible Use of Information Technology (Student) - refer to this

document for guidelines for responsible use of WSU network.

Responsible Use of University Computing Resources – WrightWay Policy number*: 3002* – refer to this document for guidelines for responsible use of Wright State University computing resources.

World Wide Web Policy - refer to this document for guidelines applicable to Web services.

Computer Account Application - refer to this document for required client information.

Guidelines for Protected Information – refer to this document for guidelines on computing habits & protected information.

Minimum Security Standards for WSU Networked Devices – refer to document for guidelines on minimum standards required for devices connected to the University network.

Password Management Policy – refer to this document for information on general password policies applicable for network, system resources, and Internet access.

Required Virus/Spyware Updated Software Policy – refer to this document for information on antivirus and spyware software requirements.

Virtual Private Network (VPN) Policy

Do It Wright - Six Quick Strategies for IT Security – refer to this guide for information on strategies to keep information assets secure.

Procurement Card Policies and Procedures – WrightWay Policy number: 5901 – refers to PCI-DSS requirements and procedures for cash collection.