University Policy 117

Information Security Policy

Initially Approved:
Policy Topic: Information Security
Administering Office: Office of CIO
Approved June 24, 2013

I. POLICY STATEMENT

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, disruption or distribution regardless of the form the data may take (electronic, paper, etc...).

Institutional information is both a valuable asset and a potential liability to the University. As such, the stewardship and security of institutional information are important responsibilities for every member of Western Carolina University (hereinafter "University" or "WCU") that has access to it. As an academic institution we must encourage the free flow of most information, while protecting critical institutional information.

The purpose of this policy is to:

A. Define information security, its overall objectives and scope and the importance of security as an enabling mechanism for institutional information sharing;
B. State the commitment of University leadership to support the goals and principles of information security;
C. Provide a framework for referencing supporting security policies; and
D. Define who is responsible for ensuring that institutional information is handled in an appropriate manner and the procedures for reporting information security incidents.

II. SCOPE AND APPLICATION OF THE POLICY

A. This policy applies to all University workforce members and any other person utilizing any form of University information technology, or having responsibility for institutional information stored in an alternate format, such as paper.
B. The Policy is an overarching information security policy that refers to a group of more specific related Information Security policies.

III. DEFINITIONS

A. Information Security – preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

B. Institutional Information – Information generated, collected, maintained and/or owned by the University regardless of format.

C. ISO 27002 - an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled *Information technology - Security techniques - Code of practice for information security management*.

D. Information Owner – The individual or department that makes decisions regarding how to define, process and handle institutional information.

E. Workforce Member – includes, but is not limited to, faculty, staff, employees, guests, consultants, vendors, volunteers, interns, student workers or temporary workers associated with the University.

IV. UNIVERSITY COMMITMENT

The following is an excerpt from the WCU Board of Trustees resolution adopted December 9, 2011:

WHEREAS, The University of North Carolina Information Technology Security Council recommended, and the University of North Carolina Chief Information Officers Council has approved, the adoption of ISO/IEC 27002 *Information Technology – Security Techniques – Code of practice for information security management* (the "ISO Standards") as the common security framework to be used by the University and other University of North Carolina constituent institutions in the development of information technology security policies; and

WHEREAS, the ISO Standards provide a comprehensive and systematic approach to ensure that appropriate information technology security controls are in place as well as flexibility to meet the specific needs of the constituent institutions; and

BE IT RESOLVED, that this Board of Trustees hereby approves the adoption of the ISO Standards as the security framework for the University.

V. SECURITY POLICY FRAMEWORK

The University of North Carolina and WCU have adopted the ISO 27002 security standard as the framework for university information security policy. As the University's IT Division and Data Security and Stewardship Committee policies existed prior to adopting this standard there are various policy numbering and naming schemes in use. This policy is the umbrella University information security policy that will refer to existing and future policies and standards that support it. Existing university policies will reference security category numbers from the ISO 27002 framework. Other existing IT security policies and future IT security policies will utilize the ISO 27002 policy numbering scheme.

VI. RESPONSIBILITIES

A. The Chancellor, Provost, Vice Chancellors, General Counsel, the CIO, the Chief of Staff and the Director of Athletics are responsible for ensuring the appropriate handling of the institutional information produced and managed by their division/unit. These positions are the institutional Data Stewards.

B. The Information Technology Division is responsible for ensuring that the appropriate technologies and system policies and permissions are in place to ensure appropriate access to electronic data.

C. The Chancellor has established a Data Security and Stewardship Committee, which reports to the Chancellor. The charge of this Committee is to oversee the implementation of this policy, ensure procedures are up to date, coordinate all relevant security policy reviews, and assist offices with risk assessments, etc.

D. Department managers are responsible for all initial and recurring security incident policy training of workforce members, and for enforcing computer and data security policies.

E. All workforce members are responsible for reporting computer security incidents and assisting the Computer Security Incident Response Team in investigating and mitigating computer security incidents.

VII. COMPLIANCE

All workforce members are:

A. Responsible for protecting any institutional information and systems that they access, process or handle;

B. Responsible for the consequences of their decisions and actions associated with institutional information access and processing; and

C. Responsible for discussing and reporting any suspicious or harmful behavior and activity to the IT Division and the owner of the institutional information, if known.

VIII. REFERENCES

International Standards Organization (ISO/IEC 27002, 5.1.1)

University Policy 97, “Data Security and Stewardship” http://www.wcu.edu/about-wcu/leadership/office-of-the-chancellor/university-policies/numerical-index/university-policy-97.asp

University Policy 106, “Identity Theft Prevention Program” http://www.wcu.edu/about-wcu/leadership/office-of-the-chancellor/university-policies/numerical-index/university-policy-106.asp