

Central Washington University

Security Services Department Strategic Plan - 2014

Author: CWU Security Services

Approval

Name	Title	Signature	Date	Rev. #
Andreas Bohman	CISO		2/26/2014	1.5

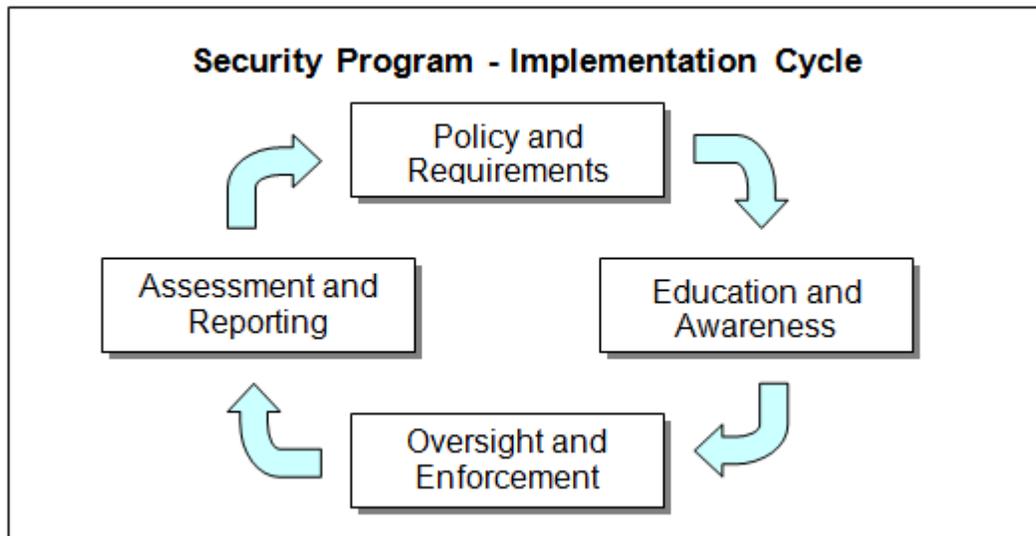
PURPOSE

The purpose of this document is to detail the Security Services strategic plan and provide a unifying vision and comprehensive overview of our strategy in providing for the confidentiality, integrity, and availability of our institutions information infrastructure. This document also summarizes the strategic plan for launching an information security program across its academic and administrative campuses. The plan is presented as a set of goals for program implementation and oversight in support of the University’s five core themes:

- Teaching and Learning
- Inclusiveness and Diversity
- Scholarship and Creative Expression
- Public Service and Community Engagement
- Resource Development and Stewardship

It is important to note that establishing an information security program is not a one-time event, but an ongoing venture that follows a cyclical process. The implementation phases are not cleanly separated processes, but instead represent a flow of activities that yield an ever maturing security program (see Figure 1). The implementation cycle involves establishing information security requirements, educating people about their responsibilities under those requirements, building governance structures to ensure program compliance, and monitoring and reporting of progress.

Figure 1



MISSION

In support of Central Washington University’s vision to prepare students for lifelong learning, the Chief Information Security Officer (CISO) and the Security Services department will establish and maintain a comprehensive and inclusive information security framework. This framework will be based on best-practice and industry standards in order to provide for the confidentiality, integrity, and availability of the University’s information infrastructure

VISION

The Security Services Department is committed to establishing a culture of information assurance and privacy at our institution by combining technology, risk management, information security, and business processes into a comprehensive and campus-wide framework. Our vision establishes information security as a provider of services and guidance to our institution's faculty, staff, and students in accordance with all applicable policies, compliance requirements, and laws.

VALUES

All staff in the Security Services department are guided by the University's core values:

Student success: CWU believes that student success is best achieved by providing supportive learning and living environments that encourage intellectual inquiry, exploration, and application. CWU believes that learning is best achieved in small classroom or group settings with ample opportunities for individualized instruction, mentoring, advising, and programming.

Access: CWU believes in providing educational opportunities to as many qualified students as possible. CWU believes that restrictions of place, time, and finances can be overcome through the effective use of partnership with community colleges and by effective and efficient use of learning, communication, and social technologies.

Engagement: CWU believes that learning, research, and creative expression are enhanced by engagement with external partners. CWU believes that as a publicly-funded institution, it has a responsibility to help address the social and economic challenges faced by our communities.

Inclusiveness: CWU believes that diversity of peoples, cultures, and ideas is essential to learning, discovery, and creative expression. CWU believes that all faculty, staff, and students must be and must feel physically, professionally, and emotionally safe in order to fully engage in and benefit from the university experience.

Shared governance: CWU believes that shared governance is most effective when information systems and decision-making processes are both robust and transparent. CWU believes that communication channels should be open and two-way and that faculty, staff, and students should be empowered to participate in the governance systems.

Facilities: CWU believes that state-of-the-art, safe, and attractive facilities enhance the working and learning environments of faculty, staff, and students. CWU also believes that state-of-the-art technologies provide leverage for the efforts of faculty, staff, and students.

Safety: CWU believes it has a responsibility to providing a working and learning environment that is both physically and emotionally safe. CWU believes this responsibility extends to the off-campus environment of its full-time, residential students.

INFORMATION SECURITY DEPARTMENT OBJECTIVES

OBJECTIVE 1: Establish an information security program

The security services department is a new operational business unit within our institution. As such, it is establishing itself as a service-oriented department with a clear focus on the confidentiality, integrity, and availability of all institutional information. In support of this objective and in alignment with the University's core theme of inclusiveness and diversity the security services department will:

- lead efforts to develop, approve, and promote an inclusive information security program based on the ISO/IEC 27001 information security management system; and
- develop policies and procedures in collaboration with the major University stakeholders in order to formally establish the University's security program.

OBJECTIVE 2: Ensure all faculty, students, and staff are aware of their information security responsibilities

In support of the University's core theme of teaching and learning, the Security Services department will ensure all employees are aware of their information security responsibilities. A robust and enterprise-wide awareness and training program is paramount to ensuring that people understand their information security responsibilities, organizational policies, and how to properly use and protect the technology resources entrusted to them. In addition, the Security Services department is committed to supporting the University's core theme of public service and community engagement.

In support of this objective, the Security Services department will:

- provide all staff, faculty, and students with the appropriate information security awareness training; and
- partner with major University stakeholders to foster a culture of information security accountability and awareness; and
- establish partnerships with the local community to provide opportunities for learning and collaboration.

OBJECTIVE 3: Establish an information security governance structure

The purpose of information security governance is to ensure our institution is proactively implementing appropriate information security controls to support the University's core theme of resource development and stewardship, while managing evolving information security risks. As such, information security governance has its own set of requirements, challenges, activities, and types of possible structures. Information security governance has a defining role in identifying key information security roles and responsibilities, and it influences information security policy development and oversight and ongoing monitoring activities.

In support of this objective, the security services department will:

- establish responsibilities for information security;
- define key information security roles and responsibilities;
- identify minimum information security controls; and
- specify compliance reporting rules and procedures.

References:

National Institute of Standards and Technology, Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*.

National Institute of Standards and Technology, Special Publication 800-100, *Information Security Handbook: A Guide for Managers*.

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001:2013 – *Information technology – Security techniques – Information security management systems – Requirements*.