Cybersecurity Roles and Responsibilities Policy

Responsible Office: Office of the CIO

I. POLICY STATEMENT

This policy defines the roles and responsibilities necessary to facilitate the management and safeguarding of Auburn University data and information systems through effective control processes.

All Auburn University users and units are responsible for the security of information within their control and for complying with all State and Federal Regulations, and Auburn University Cybersecurity policies, procedures and guidelines.

This policy is intended to guide the establishment and documentation of cybersecurity control capabilities throughout Auburn University IT units and Application Owners to assure Auburn University implements cybersecurity best practices.

II. POLICY PRINCIPLES

OIT maintains the Auburn General System Security Plans (SSP) for systems they control. Examples include: the Auburn Data Network, Active Directory, Multi-factor authentication and Core Administrative Systems such as Banner Student, Canvas, and Email.

Application Owners (colleges, departments or individual users) are responsible for establishing, maintaining and documenting security controls for all IT systems and data they control. This would include applications utilized by a specific college or department. In the event of a failure of these controls, the Application Owners are responsible for any remediation activities that may arise.

When an application/ IT System maintains confidential information as specified by the Data Classification Policy, the Application Owner will be required to create a written Systems Security Plan (SSP). An SSP will also be required when called for by contractual requirements, research grant/proposal requirements, or due to regulatory requirements, including but not limited to HIPAA, GLBA, Cybersecurity Maturity Model Certification (CMMC) and PCI-DSS.

Typically, documenting a System Security Plan (SSP) and developing, implementing and monitoring controls is a collaborative effort by the Office of Information Technology (OIT), Application Owners, Distributed Information Technology (DIT) and the Cybersecurity Office.

When purchasing software which maintains Confidential Information (Data Classification Policy), the creation of an SSP, which has been reviewed and approved by the Office of Cybersecurity is required prior to using data in test and a final review is required prior to the move to production.

III. DEFINITIONS

Access: Ability to make use of any information system (IS) resource. Source: CNSSI 4009, NIST SP 800-32, NIST SP 800-161

Access Control: The process of granting or denying specific requests to: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities. Source: FIPS 201, CNSSI 4009

Application: The system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications. NIST SP 800-16

A system for collecting, saving, processing, and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed. The terms application and software application are often used synonymously. NISTIR 7695

Auburn University Application Owners (Entities): Any individual or group at Auburn University with the responsibility to ensure that the program or programs, which make up the application, accomplish the specified objective or set of user requirements established for that application, including appropriate security safeguards. For Auburn, Application Owners are typically responsible for applications utilized in their specific colleges, departments or by individual users.

Auburn University IT Unit: Any IT entity that is responsible for the management, operation, and security of Auburn University IT resources, to include systems, applications, IT infrastructure, and data. For Auburn University, this includes the Office of Information Technology (OIT), Distributed Information Technology (DIT) units, and departments and users that maintain their own IT capabilities.

Authentication: A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information. Source: CNSSI No. 4005

Capability: Capabilities are achievements to ensure cybersecurity objectives are met within each domain. Capabilities are met through the employment of practices and processes. Each domain is comprised of a set of capabilities. Source: CMMC

Least Privilege: A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs. Source: NIST SP 800-57 Part 2

IT System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. NIST SP 800-171 Rev. 1

System Security Plan: The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. Source: CNSSI 4009

System Software: Computer software used to control and coordinate the computer hardware and to provide an environment for executing application software.

IV. GLOSSARY

CMMC: Cybersecurity Maturity Model Certification

CNSSI: Committee on National Security Systems Instruction

CUI: Controlled Unclassified Information

DIT: Distributed Information Technology

FERPA: Family Educational Rights and Privacy Act

FIPS: Federal Information Processing Standards

GLBA: Gramm-Leach-Bliley Act

HIPAA: Health Insurance Portability and Accountability Act

NIST: National Institute of Standards and Technology

OIT: Office of Information Technology

PII: Personally Identifiable Information

PCI-DSS: Payment Card Industry – Data Security Standards

SSP: System Security Plan

V. EFFECTIVE DATE

August 25, 2020

VI. APPLICABILITY

This policy applies to all employees, contractors, vendors, or anyone using Auburn University owned or operated Information Technology (IT) resources, which includes information that is processed, transmitted, or stored, on behalf of Auburn University, either on premise or cloud based.

VII. POLICY MANAGEMENT

Responsible Office: Office of the Chief Information Officer
Responsible Executive: Chief Information Officer
Responsible Officer: University Chief Information Security Officer

VIII. ROLES and RESPONSIBILITIES

The Chief Information Security Officer (CISO) is responsible for:

1. Ensuring that appropriate control policies, plans, and procedures are developed, maintained,

published, and disseminated for Auburn University assets.
2. Assisting all affected Auburn University IT Units develop, adopt, or adhere to formal, documented procedures that address purpose, scope, roles, responsibilities, management, and coordination among organizational entities.

Application Owners, Individuals, OIT and Auburn University IT Units are responsible for:

1. Creating System Security Plans (SSP) for confidential data they control. The System Security Plans should include, but not be limited to:
    a. Adhering to Auburn University security standards, policies and procedures.
    b. Limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). (User Access)
    c. Utilizing Auburn's single sign-on solution and two-factor authentication whenever possible.
    d. Limiting information system access to the types of transactions and functions that authorized users are permitted to execute. (System Access)
    e. Establish audit trail and audit trail processes that alert and record access, modification and download of information deemed as Confidential. (See Data Classification Policy)
    f. Controlling the flow of confidential and operational data (PII, PCI-DSS, CUI) in accordance with approved authorizations.
    g. Separating the duties of individuals to reduce the risk of malevolent activity without collusion.
    h. Employing the principle of least privilege, including for specific security functions and privileged accounts.
    i. Enforcing designated limit of consecutive invalid logon attempts by a user during a designated period.
    j. Employing proper system notification messages and/or banner displayed before individuals log into systems.
    k. Employing session lock capability with pattern-hiding displays to prevent access/viewing of data after period of inactivity.
    l. Employing a mechanism to ensure termination of user-initiated logical sessions.
    m. Providing a means to associate Auburn University-defined types of security attributes with data/information in storage, in process, and/or in transmission.
    n. Monitoring and controlling remote access sessions.
    o. Protecting wireless access using authentication and encryption.
    p. Controlling the connection of mobile devices.
    q. Verifying and controlling connections to and use of external information systems.
    r. Facilitating information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for the cases where user discretion is required.
2. Understanding the regulations that govern their area and documenting steps taken to reach compliance in such areas as FERPA, HIPAA, GLBA, Research Contracts, etc.
3. Support is available from the Auburn University Cybersecurity Office.

VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy is subject to disciplinary action, up to and including dismissal.

Systems implemented without proper approval from the Office of Cybersecurity are subject to being removed.

IX. COMPLIANCE GUIDELINES

1. Cybersecurity Maturity Model Certification (CMMC), Department of Defense
2. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
3. NIST Cybersecurity Framework (CSF), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,
4. NIST Special Publication (SP) 800-171 Revision (Rev) 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, U.S. Department of Commerce National Institute of Standards and Technology (NIST)
5. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
6. Payment Card Industry Data Security Standard (PCI-DSS)

X. EXCLUSIONS

None.

XI. INTERPRETATION

The Auburn University Chief Information Officer has the authority to interpret this policy.