SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

1.0 STANDARD FOR PROTECTION OF TEST DATA

1.1 PURPOSE
The purpose of this standard is to establish the university’s obligation to ensure the protection of data used for testing.

1.2 SCOPE
It is the responsibility of any party working with test data within the University environment to understand and apply information security rules to ensure appropriate security for that data.

1.3 CONTROL OBJECTIVE
To ensure the protection of data used for testing.

1.4 STANDARD
Protection of test data
The use of production data containing personally identifiable information, confidential or otherwise sensitive data for testing should be avoided. If that data must be used, access controls and other securities in place for the production system should also be applied to the test system.

These requirements should be considered when using production data for testing purposes:

- Copying production information to a test environment requires documented authorization every time that information is copied.
- When practical, production information should be erased from a test environment immediately after the testing is complete.
- An audit trail should be maintained to log the copying and use of production information.

1.5 RELATED RESOURCES
ISO/IEC 27002: 14.3
Direct your questions about this standard to DIT Information Security Office at infosec@ecsu.edu.

1.6 REVISION HISTORY

Approved by DIT Security Committee 12-2017
2.0 STANDARD FOR SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

2.1 PURPOSE
The purpose of this standard is to establish the university’s obligation to ensure that information security is designed and implemented within the development lifecycle of information systems.

2.2 SCOPE
It is the responsibility of any party considering development of an information system within the University environment to understand and apply information security rules which ensure appropriate security for the system.

2.3 CONTROL OBJECTIVE
To ensure that information security is designed and implemented within the development lifecycle of information systems.

2.4 STANDARD
Secure development
Secure development is critical for building any secure service architecture, software or system. These requirements should be considered:

- Documented agreement on access levels (i.e., end user, privileged, administrative, etc.) and corresponding authorization requirements
- Submission of change requests only by authorized users
- Reviews to ensure controls and integrity procedures are not compromised by change
- Identification of all software, information, database entities and hardware involved in or impacted by change
- Security review to minimize likelihood of known security weaknesses
- Formal approval prior to commencement of work
- Authorized user acceptance prior to implementation
- System documentation updates
- Version control for all software updates
- Audit trail of all change requests
Operating documentation and user procedures changed as needed to remain current
Timing of change to prevent or minimize business impact

Technical review of applications after operating platform changes
When operating platforms including operating systems, databases and middleware platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. The following should also be considered:
- Review of application control and integrity procedures to ensure they have not been compromised by change to the operating platform
- Notification of change with enough lead time to allow appropriate tests and reviews prior to implementation

Restrictions on changes to software packages
Modifications to vendor supplied software packages is discouraged and limited to necessary changes. All changes should be strictly controlled. The following should be considered:
- Risk of compromise of built-in controls and integrity processes
- Possible need for consent from vendor
- Possibility of obtaining required changes from vendor as standard program updates
- Impact if the university becomes responsible for future maintenance of software as a result of changes
- Compatibility with other software in use
- Maintaining original software and making changes to designated copy

Secure development environment
A secure development environment includes people, processes and technology associated with system development and integration. Risks associated with individual system development efforts should be assessed and secure development environments established with the following considerations:
- Sensitivity of data to be processed, stored and transmitted by the system
- Applicable external and internal requirements, e.g., from regulations or policies
- Security controls already implemented by the university that support system development
- Trustworthiness of personnel working in the environment
Degree of outsourcing associated with system development
Need for segregation between different development environments
Control of access to development environment
Monitoring of change to the environment and code stored therein
Storage of backups at secure offsite location
Control over movement of data to and from the environment

**Outsourced development**

Where a system is outsourced, the following points should be considered:

- Licensing arrangements, code ownership and intellectual property rights related to the outsourced content
- Contractual requirements for secure design, coding and testing practices
- Agreement of an approved approach for analyzing the security of the application
- Acceptance testing for quality and accuracy of deliverables
- Agreement on minimum acceptable levels of security and privacy quality
- Agreement on evidence that sufficient testing has been applied to ensure the absence of intentional and unintentional malicious content upon delivery
- Contractual rights to audit development processes and controls
- Comprehensive documentation of the build environment used to create deliverables

**System security testing**

Security functionality should be tested throughout the development process and should include a detailed schedule of activities and expected results under a range of conditions.

**System acceptance testing**

Acceptance testing and criteria should be established for new information systems, upgrades and new versions. The following should be considered:

- Testing of information security requirements
- Testing of received components and integrated systems
- Use of code analysis tools and vulnerability scans to verify remediation of security-related defects
- Use of test environment which ensures realistic approximation of the university environment without introducing vulnerabilities into the production environment
2.5 RELATED RESOURCES

ISO/IEC 27002: 14.2

Direct your questions about this standard to DIT Information Security Office at infosec@ecsu.edu.

2.6 REVISION HISTORY

Approved by DIT Security Committee 12-2017
3.0 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

3.1 PURPOSE

The purpose of this standard is to establish the university’s obligation to ensure that information security is integrally tied to all university information systems throughout the life of any given system including any information systems which provide services over public networks.

3.2 SCOPE

It is the responsibility of all information system owners to ensure that security controls are considered for their information systems throughout the lifecycle, from initial planning to service retirement.

3.3 CONTROL OBJECTIVE

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

3.4 STANDARD

Prior to implementation or enhancement

Information security requirements should be included in the considerations for any new information system or for the enhancement of any existing information system. For acquired systems/services, security requirements should be fully addressed in the contract and any risks considered prior to purchase. Use of the university’s centrally managed authentication services is required. If an information system is unable to integrate with the centrally managed authentication services, an official exception must be approved by DIT.

The following requirements should be addressed:

- User authentication requirements
- Access provisioning
- Authorization processes (for end users and privileged accounts)
- Communicated guidelines regarding user responsibilities when accessing the system
- Protection of any associated data or assets including the availability, confidentiality and integrity of those assets
- Other security control mandates such as required interfaces to logging and monitoring systems
NOTE: The following checklists provide a starting point to review information security related to systems and services:

- Information Security Checklist
- Information Security Checklist for Externally Hosted Services

*Services provided via the Internet or other public network*

Extra care must be taken to protect information involved in application services which pass over the Internet or other public networks. That care should include protection from fraudulent activity, contract dispute, and unauthorized disclosure or modification.

NOTE: Any application involving payment transactions should be coordinated through the University Controller’s office and comply with the Payment (Credit/Debit) Card Processing Standard

*Protecting application services transactions*

Information involved in application service transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

### 3.5 RELATED RESOURCES

ISO/IEC 27002: 14.1

Direct your questions about this standard to DIT Information Security Office at infosec@ecsu.edu.

### 3.6 REVISION HISTORY

Approved by DIT Security Committee 12-2017