Florida Agricultural & Mechanical University
Board of Trustees Policy

Board of Trustees Policy Number: 2008-01a	Date of Adoption/Revision: March 20, 2008

Subject	**ENTERPRISE INFORMATION SYSTEMS SECURITY AND CONTROLS**
Authority	Section 282.318, F.S., Chapter 815, F.S. Florida Computer Crimes Act, 18 U.S.C., 1030, Fraud and Related Activity in Connection with Computers, *16 CFR Part 314*
Applicability	**University**

I. Policy Statement and Purpose

Information Technology (IT) tools are vital to the University operations and to the improvement of the quality and efficiency of our work. As repositories for critical and sometimes highly proprietary University community information, to allow improper access, disruption, or the destruction of these resources would create grave consequences for the University. Therefore, the purpose of this document is to communicate the University's IT policy to the University community of stakeholders, including, but not limited to faculty, students, staff, service providers, vendors and alumni/community. It is the policy of Florida A&M University to protect the confidentiality of and to:

- Ensure the University community IT resources are appropriately protected from destruction, disruption, alteration or unauthorized access, disclosure and misuse of information.
- Ensure that IT resource protections are accomplished in a manner consistent with the business and workflow requirements of the University and best practices of the industry.
- Ensure the security and confidentiality of individual stakeholder's information as defined in 16 CFR Part 314; protect against any anticipated threats or hazards to the security or integrity of such information; and, protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any individual stakeholder.

Federal or State laws, rules, regulations, policies, and procedures governing the confidentiality of data are not superseded, abridged, or amended by this policy.

II. Definitions

Information Technology – Information Technology (IT) includes, but are not limited to the following university resources:

- Computer hardware and peripherals
- Communication closets
- Telephony
- Life Safety systems, e.g. IP based cameras, doors, notification systems ,etc
- Software
- Electronic data stored on standalone devices, networks, diskettes, databases, etc.
- Network infrastructure equipment and/or devices
- The University Intranet and access to and data transmissions across the Internet and World Wide Web.
-

Chief Information Officer (CIO) – The Chief Information Officer is the central point of and controlling factor for electronic information maintained and used by the University for the operation, planning, research, forecasts, and educational programs.

III. Procedures, Approvals/Responsibilities

The Chief Information Security Officer shall be responsible for implementing the following policies and performing the following duties:

1. Develop Procedures/Policies

   Develop and periodically update written internal policies and procedures to assure security of the data and information technology resources. The internal policies and procedures which, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from the provisions of Chapter 119, Florida Statutes. Develop policies and procedures that recognize that sensitive or critical resources require special protection.

2. Data Classification

   Create classification system on current information determined to be sensitive or confidential and procedures on how to access that information.

3. Conduct Reviews

   a. Conduct and update periodically a comprehensive risk analysis to determine the security threats to the data and information technology resources. The risk analysis information is confidential and exempt from the provisions of Chapter 119, Florida Statutes. Risk analysis results will be presented to the owner of the information resource for risk management.

   b. Perform internal reviews of the information technology resources security function. This will be done periodically, when there are major system changes, or as directed by appropriate management. The results of such internal reviews and evaluations are confidential information and exempt from the provisions of Chapter 119, Florida Statutes.

4. Implement Access Controls

   a. Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from the identified risks to the data and information technology resources.

   b. Ensure that media which contain sensitive or confidential information is accessed only by authorized personnel as required in the performance of their duties.

   c. When confidential or sensitive information is transferred from one location to another in the transaction of official business, ensure that the personnel receiving the information are individuals responsible for maintaining the confidentiality of the information in accordance with the conditions imposed by the originating location. Define procedures for the transfer of this information that will provide for an auditable chain of custody.

   d. Ensure that data or information resources are free of sensitive or confidential information before being disposed of from or removed from EIT security controls.

   e. Establish access controls for information processing areas that are appropriate for the size and complexity of the operations and the criticalness or sensitivity of the systems operated at those locations.

   f. Ensure that data integrity controls to sensitive, confidential, or critical data are implemented and that only legitimate users have access to these resources. Controls will ensure that this information is protected from erroneous, fraudulent, or unauthorized access and modification. Establish audit trails for access.

g. Require the owners, in consultation with the custodians of data, to determine what data need to have regular copies made for recovery purposes, in what form, and how often.

h. Include appropriate security requirements in written specifications for the solicitation of information technology resources.

5. Maintain Disaster Recovery Plan

Ensure that all information resource owners, custodians, and all automated user functions identified as critical to the continuity of operations, as determined by risk analysis, have a written and cost effective contingency plan that provides prompt and effective continuation of critical missions in the event of a disaster.

Chief Information Officer (CIO)

The Chief Information Officer (CIO) is responsible for the implementation of this policy.

Chief Information Security Officer (CISO)

The Chief Information Security Officer reports to the CIO. The CISO has primary responsibility for the oversight of the state of information security at the University and is charged with the definition of security strategy and scope. Primary responsibilities include:

a. Develop and periodically update written internal policies and procedures to assure security of the data and information technology resources. The internal policies and procedures which, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from the provision of Chapter 119, Florida Statutes.

b. Develop policies and procedures that recognize that sensitive or critical resources require special protection.

c. Reporting on the state of information security.

d. Performing oversight of the security efforts of area managers, network engineers, security engineers and other security related specialists as appropriate; insuring adherence to operations related security policies and procedures.

e. Serving as primary point of contact for auditors during formal audit processes.

f. Preparing formal responses and action plans pursuant to internal audits.

g. Identifying and recommending individuals responsible for security engineering functions outsourced.

h. Reviewing operations related to security.

i. Identifying and establishing disaster recovery and business continuation/continuity plans for all critical systems.

j. Performing periodic risk assessments based on industry standards included by reference and will be complied with except where superseded by University approved procedures.

k. Evaluating and adjusting the University information security program in light of its annual risk assessment and regularly provide security performance metrics.

l. Providing adequate Security Awareness Training for University employees and students.

System Administrator Authority

a. System administrative privileges shall be limited to those support personnel requiring them for business purposes. Such authority shall be revoked upon determination by Enterprise Information Technology (EIT) Security management that such access is no longer required.

b. EIT Security shall be responsible for maintaining a current roster of individuals with administrative accesses to each supported system or set of systems.

University Employees, Contractors and Students

a. University employees, contractors and students are responsible for complying with this policy and as such must receive Security Awareness Training.
b. Managers are responsible for ensuring that their staff and/or contractors comply

with this policy.

c. Managers will include information security as part of their employee and/or contractor orientation.

Procedure

The Chief Information Security Officer shall be responsible for implementing the following policies and performing the following duties:

6. Develop Procedures/Policies

   Develop and periodically update written internal policies and procedures to assure security of the data and information technology resources. The internal policies and procedures which, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources are confidential information and exempt from the provisions of Chapter 119, Florida Statutes. Develop policies and procedures that recognize that sensitive or critical resources require special protection.

7. Data Classification

   Create classification system on current information determined to be sensitive or confidential and procedures on how to access that information.

8. Conduct Reviews

   a. Conduct and update periodically a comprehensive risk analysis to determine the security threats to the data and information technology resources. The risk analysis information is confidential and exempt from the provisions of Chapter 119, Florida Statutes. Risk analysis results will be presented to the owner of the information resource for risk management.

   b. Perform internal reviews of the information technology resources security function. This will be done periodically, when there are major system changes, or as directed by appropriate management. The results of such internal reviews and evaluations are confidential information and exempt from the provisions of Chapter 119, Florida Statutes.

9. Implement Access Controls

   a. Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from the identified risks to the data and information technology resources.

   b. Ensure that media which contain sensitive or confidential information is accessed only by authorized personnel as required in the performance of their duties.

   c. When confidential or sensitive information is transferred from one location to another in the transaction of official business, ensure that the personnel receiving the information are individuals responsible for maintaining the confidentiality of the information in accordance with the conditions imposed by the originating location. Define procedures for the transfer of this information that will provide for an auditable chain of custody.

   d. Ensure that data or information resources are free of sensitive or confidential information before being disposed of from or removed from EIT security controls.

   e. Establish access controls for information processing areas that are appropriate for the size and complexity of the operations and the criticalness or sensitivity of the systems operated at those locations.

   f. Ensure that data integrity controls to sensitive, confidential, or critical data are implemented and that only legitimate users have access to these resources. Controls will ensure that this information is protected from erroneous, fraudulent, or unauthorized access and modification. Establish audit trails for access.

   g. Require the owners, in consultation with the custodians of data, to determine what data need to have regular copies made for recovery purposes, in what form, and how often.

   h. Include appropriate security requirements in written specifications for the solicitation of information technology resources.

10. Maintain Disaster Recovery Plan

    Ensure that all information resource owners, custodians, and all automated user functions identified as critical to the continuity of operations, as determined by risk analysis, have a written and cost effective contingency plan that provides prompt and effective continuation of critical missions in the event of a disaster.

Compliance

Standards

All policies created shall conform to industry standards including, but not limited to Payment Card Industry (PCI), Sarbanes-Oxley (SOX), Family Educational Rights and Privacy Act (FERPA), and Health Insurance Portability and Accountability Act (HIPAA) where applicable.

Enforcement

Actions that are illegal or against university policy will be referred to the appropriate officials regardless of whether or not a computer was involved in their commission. EIT role is to provide technical assistance to the authorities. Only minor computer and network policy violations will be handled internally by EIT.

EIT may monitor user activities and access any files or information in the course of performing normal system and network maintenance or while investigating policy or violations. Anyone using EIT resources expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, EIT will provide the evidence to law enforcement officials.

Offenders may be prosecuted under laws including (but not limited to):

- The Privacy Protection Act of 1974
- The Computer Fraud and Abuse Act of 1986
- The Computer Virus Eradication Act of 1989
- The Electronic Communications Privacy Act 1986
- CDA-Communications Decency Act - 1996
- Web Copyright Law – 1997
- COPA - Child Online Protection Act – 1998
- Digital Millennium Copyright Act - October 28, 1998
- HIPPA – Health Insurance and Portability Act - 1996

Disciplinary Actions

A. Suspected violations of this policy should be reported to the Chief Information Officer and the Information Security Manager.
B. Individuals who violate this policy will be subject to discipline as appropriate.
C. The University has primary responsibility and authority for all components of the IT infrastructure. All devices, applications, databases and other components must comply with the university policies.

D. The University information security cooperates with law enforcement agencies in their efforts to investigate any violation of federal and state laws. If the University suspects the violation of any law, the University may ask campus police or an external law enforcement agency to investigate the matter.
E. Users reasonably believed by the University to have willfully compromised its information security are subject to investigation, possible prosecution and/or termination/dismissal.
F. An employee who interferes with or refuses to cooperate in the investigation of violation of this policy will be subject to discipline, possible prosecution and/or termination/dismissal.
G. A student who interferes with or refuses to cooperate in the investigation of violation of this policy will be subject to discipline, possible prosecution and/or termination/dismissal.
H. Business units or departments may establish additional procedures that are relevant to their operations providing that these additional procedures:
    i. Do not conflict with this policy,
    ii. Provide specific operational detail, and

    Are more restrictive in security posture.