FOUNTAINHEAD
College of Technology

Information Assurance Policy for Information Systems

1. Purpose 3

2. Goals 3

3. Applicability 4

4. Compliance 4

5. Roles & Responsibilities 4

5.1. All Departments 4

5.2. FCT Information Systems Security Officer (ISSO) 4

5.3. Computing and Network Services (CNS) 5

5.4. FCT Center for Information Assurance & Cybersecurity Training (IACT) 6

5.5. System Owners and Operators 7

5.6. Data Custodians 8

5.7. Users 8

6. Policy 9

6.1. General Statement of Policy 9

6.2. Monitoring User Accounts, Files and Access 9

6.3. Electronic Data and Records Management 10

6.4. Access Controls 10

6.5. Systems and Network Security 11

6.6. Physical Security 12

6.7. Personnel Security Measures 12

6.8. Policy Enforcement 14

6.9. Policy Maintenance 14

1. Purpose

Fountainhead College of Technology (FCT) is a proprietary institution with custodial responsibilities for a significant and diverse amount of sensitive information. This role places significant responsibilities on FCT regarding the management and use of its information systems resources.

This document establishes FCT's information assurance policy for information systems. The information assurance policy for information systems is intended to protect the integrity of campus networks and to mitigate the risks and losses associated with security threats to campus networks and information systems resources.

Attacks and security incidents constitute a risk to FCT's academic mission. The loss or corruption of data or unauthorized disclosure of information on research and instructional computers, student records, and financial systems could greatly hinder the legitimate activities of the college staff, faculty and students. The college also has a legal responsibility to secure its computers and networks from misuse. Failure to exercise due diligence may lead to financial liability for damage done by persons accessing the network from or through the college. Moreover, an unprotected college network open to abuse might be shunned by parts of the larger network community. This policy will allow FCT to handle information systems security responsibly.

The purpose of this policy is to help ensure the security, and availability of information technology systems and networks and the confidentiality, integrity, proper authorization and non-repudiation of electronic information captured, maintained, and used by FCT. This policy provides direction for compliance with federal and state regulations, specifies appropriate practices, and defines custodial responsibilities for confidential records associated with FCT operations. This policy should be used as the foundation document for all standards, procedures, and guidelines that are developed and implemented by FCT related to information systems and data security.

This policy is subject to revision and will be valuated as FCT gains experience with this policy.

2. Goals

The goals of this information assurance policy for information systems are to:

Establish institution-wide policies to protect the college's networks and information systems from abuse and inappropriate us.

Establish mechanisms that will aid in the identification and prevention of abuse of college networks and information systems.

Provide an effective mechanism for responding to external complaints and queries about real or perceived abuses of college networks and information systems.

Establish mechanisms that will protect the reputation of the college and will allow the college to satisfy its legal and ethical responsibilities with regard to network and information system connectivity to the worldwide Internet.

Establish mechanisms that will support the goals of other existing policies, e.g., Acceptable Use Policy and Student Rules of Conduct.

Note: Any violation of the information assurance policy for information systems will also be deemed a violation of the above listed policies, as appropriate.

3. Applicability

This policy is applicable to all users (employees, faculty, students, contractors, and others) and support personnel (system administrators, network engineers, systems engineers, and others) of FCT computing systems, networks, digital information, and any other electronic processing or communications related resources or services provided throughout FCT.

4. Compliance

Successful compliance and protection of information systems assets requires that all owners, operators, and users of FCT computing and network services and systems learn, understand, and abide by this policy.

In addition, it is the responsibility of owners and operators of computer systems and applications associated with FCT to evaluate their specific compliance requirements on a regular basis as directed by FCT security policy.

5. Roles & Responsibilities

Responsibility for protecting FCT information systems and data is shared by many entities and individuals throughout the institution including the Information Systems Security Officer (ISSO), the Center for Information Assurance & Cybersecurity Training, Computing & Network Services (CNS), and all FCT system owners, operators, data custodians, and users. The following section describes the specific roles and responsibilities of each of these groups.

5.1. All Departments

In support of this policy, all departments that administer LANs connected to the backbone will:

Provide CNS with the names, email addresses, and telephone numbers for a primary technical contact and (if applicable) an alternate contact.

Endeavor to assign to an individual the authority to connect systems to the departmental network(s).

Endeavor to keep this information up to date.

5.2. FCT Information Systems Security Officer (ISSO)

The Information Systems Security Officer (ISSO) serves as a bridge to both those responsible for technical aspects (CNS, data custodians, system operators and users) and the business and administrative issues (upper-managment and IACT) of securing information. The information assurance objectives of FCT are critical to the success of the college’s mission. FCT has appointed an ISSO as an integral component of its commitment to protect privacy and integrity, and comply with all requirements for information systems protection. The role of the ISSO is to provide strategic oversight, coordination, and implementation of the college's information assurance and compliance efforts. The ISSO is appointed by FCT’s president.

Person responsible: Tim Thomas

The success of the ISSO’s efforts depends on strong support from all system owners, operators, data custodians, and users throughout the FCT. The responsibilities of the ISSO are as follows:

Coordinate all network security efforts and act as the primary administrative contact for all related activities.

Coordinate investigations into any alleged computer or network security compromises, incidents, or problems; to ensure that this coordination is effective, security compromises should be reported to the ISSO – email: security@fountainheadcollege.com or 865-688-9422.

Cooperate in the identification and prosecution of activities contrary to college policies and the law; actions will be taken in accordance with relevant college Policies, Codes and Procedures with, as appropriate, the involvement of campus security officers or other law enforcement agencies.

Consult with system administrators in the development of procedures for handling and tracking a suspected intrusion, and the deployment of those procedures in the resolution of security incidents.

Manage and oversee the FCT Computing and Network Services (CNS).

The development, implementation, and maintenance of an institution-wide strategic information systems security plan.

The development, implementation, and enforcement of institution-wide information systems security policy and related recommended guidelines, operating procedures, and technical standards.

Manage the process of handling requested policy exceptions.

Advise upper-management on related risk issues and recommend appropriate actions in support of the FCT's larger risk management programs.

Ensure related compliance requirements are addressed, e.g., privacy, security, and administrative regulations associated with federal and state rules.

Ensure appropriate risk mitigation and control processes for security incidents as required.

5.3. Computing and Network Services (CNS)

Computing & Network Services (CNS) provides an active, key role in computer security planning, analysis, prevention, incident response, and technical education for the college community.

Persons responsible: Taylor Barnes, Network Administrator

CNS’s security responsibilities include the following:

Monitor, in real time, backbone network traffic, as necessary and appropriate, for the detection of unauthorized activity and intrusion attempts.

Carry out such monitoring in compliance with the college’s statement on Personal Privacy (*See Acceptable Use Policy: General Use and Ownership*).

Seek the cooperation of the appropriate contacts for the systems and networks involved when a security problem (or potential security problem) is identified to resolve such problems, but in the absence or unavailability of such individuals, be prepared to act unilaterally to contain the problem, up to and including temporary isolation of systems or devices from the network, and to notify the responsible system administrator when this is done.

Publish security alerts, vulnerability notices and patches, and other pertinent information in an effort to prevent security breaches.

Carry out and review the results of automated network-based security scans of the systems and devices on college networks to detect known vulnerabilities or compromised hosts.

Inform the departmental system administrators of planned scan activity, providing detailed information about the scans, including time of scan, originating machine, and vulnerabilities for which the information system(s) are being tested. The security, operation, or functionality of the scanned machines should not be endangered by the scan.

Report the results of the scans that identify security vulnerabilities only to the departmental system administrator contact responsible for those systems.

Report recurring vulnerabilities over multiple scans to departmental management.

If identified security vulnerabilities, deemed to be a significant risk to others and which have been reported to the relevant system administrators, are not addressed in a timely manner, take steps to disable network access to those systems or devices until the problems have been rectified.

Prepare summary reports of its network security activities for the ISSO on a quarterly basis.

Prepare recommendations and guidelines for network and system administrators.

Provide assistance and advice to system administrators to the extent possible with available resources.

Issue semiannual requests to verify the accuracy of departmental contact information.

Support for FCT security policy development, implementation, and enforcement.

Support for FCT strategic security planning and plan implementation.

Support for the development of security strategy in FCT information systems architecture.

Support for security and privacy awareness and education programs.

Incident response services as needed.

Computer forensic services as required.

Security consulting services as needed.

Support for the development and implementation of all appropriate standards and guidelines as necessary.

CNS coordinates its administrative activities and incident response procedures as necessary with the ISSO. In addition, it works closely with Center for Information Assurance & Cybersecurity Training (IACT) Team to ensure institution-wide service continuity and to leverage all mutually beneficial activities and resources.

5.4. FCT Center for Information Assurance & Cybersecurity Training (IACT)

The FCT Center for Information Assurance & Cybersecurity Training (IACT) plays a key role of centralized direction, and support for all information systems security-related services for FCT. The group's responsibilities include the following:

Persons responsible: John Mailen, Patrick Allen; IACT Program Coordinator

Support and guidance for FCT security policy development, implementation, and enforcement.

Support for FCT strategic security planning and plan implementation.

Development, implementation and support for security awareness and education programs.

Incident response services as needed.

Computer forensic services as required.

Security consulting services as needed.

Support for the development and implementation of all appropriate standards and guidelines as necessary within the FCT community.

The IACT works closely with the ISSO to ensure institution-wide service continuity and to leverage all mutually beneficial activities and resources.

5.5. System Owners and Operators

System owners and operators play a critical role in protecting FCT information systems and data. Their ranks might include members of the FCT professional staff, department heads, faculty members, contracted employees, or students.

System owners' and operators' areas of responsibilities for systems and information security include the following:

Comply with FCT policies and statutory and regulatory requirements.

Comply with FCT guidelines related to logical and physical security.

Comply with "Acceptable Use Policy.”

Maintain confidentiality of sensitive data, especially personally identifiable information and valuable intellectual property.

Grant access to all users based on the principle of least privilege where required.

Grant access to all users based on the principle of separation of duties where required.

Submit documented reports to the appropriate authority involving incidents of security breaches with the potential to compromise personally identifiable information.

Submit documented requests to the ISSO of any desired exceptions to FCT policy.

Perform incident response activities when incidents involve their system(s).

Specify security resources as required in college budget processes and in grant proposals.

All system owners and operators are encouraged to work closely with the ISSO, data custodians, and CNS to help ensure the successful protection of FCT computing resources and data.

5.6. Data Custodian

Data custodians are individuals who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department or administrative unit of FCT. The role of the data custodians is to provide direct authority and control over the management and use of specific information. These individuals might be department heads, managers, supervisors, or designated staff. They might serve dual roles as a system owner or operator and a data custodian.

Data custodians must follow all appropriate and related security guidelines to ensure the protection of sensitive data and intellectual property residing on systems for which they have accountability.

Data custodians' responsibilities include the following:

Ensure compliance with all FCT policies and all statutory and regulatory requirements.

Provide system owners and operators with requirements for access control measures to protect sensitive data.

Ensure appropriate disposal of all media on which data is stored at the end of its use.

Ensure appropriate security measures for transmission of data.

Support access control of data by acting as a control point for all access requests.

Support regular review and control procedures that ensure that all access privileges are current and appropriate.

Submit documented reports to the appropriate authority if there is a possibility of compromise of personally identifiable information.

Ensure that all access is granted based on the principle of least privilege where required.

Ensure that all access is granted based on the principle of separation of duties where required.

Data custodians, in conjunction with the system owners and operators and the FCT ISSO, are responsible for documenting any requested exceptions to FCT privacy protection policies. Documented exceptions must be approved in writing by the authorized college officials responsible for the electronic information to which the exception applies. Exceptions will be considered only when warranted and only to the degree necessary to achieve the mission and business needs of the college. Any and all exceptions made must be documented with the ISSO and upper-management.

5.7. Users

All users have a critical role in the effort to protect and maintain FCT information systems and data. Users of FCT computing resources and data have the following responsibilities:

Support compliance with all federal and state statutes and regulations.

Comply with all FCT policies and guidelines.

Protect against unauthorized access to accounts, privileges, and associated passwords.

Maintain confidentiality of sensitive information to which they are given access privileges.

Accept accountability for all activities associated with individual user accounts and related access privileges assigned to them.

Restrict to authorized purposes the use of FCT computers, email, computer accounts, and networks and the information accessed, stored, or used on any of these systems.

Report all suspected security and/or policy violations to an appropriate authority (e.g., manager, supervisor, system administrator, CNS, or the ISSO).

Report all known violations of privacy policy to the ISSO.

Users are also required to follow all specific policies, guidelines, and procedures established by the FCT departments or business units with which they are associated and that have provided them with access privileges.

6. Policy

The following section sets forth FCT's general policy regarding the security, availability, privacy, and integrity of its information systems, networks, and data. It stipulates specific policies for monitoring computing resources, managing electronic data and records, and controlling access to computing resources. In addition, it outlines minimum standards and practices for systems and network security.

6.1. General Statement of Policy

FCT provides information system resources to its divisions, faculty, and departments in support of its academic mission. This policy puts in place measures to prevent or at least minimize the number of security incidents on the campus information systems without impacting the academic mission or the integrity of the college's different information systems communities.

It is the policy of FCT to ensure the security, availability, privacy, and integrity of its information systems, networks, and data and to ensure full compliance with all applicable federal and state statutes and regulations.

All providers and users of FCT computing services, resources, and data are required to comply with all established policies, guidelines, and procedures, including applicable federal and state statutes and regulations.

The general policy outlined in this section is the foundation for all other policy statements, guidelines, and procedures that are developed and implemented within FCT computing environments.

6.2. Monitoring User Accounts, Files and Access

FCT may monitor equipment, systems and network traffic at any time (See *FCT Acceptable Use Policy*). The normal operation and maintenance of FCT computing and network resources require authorized FCT staff to back up and cache data and communications, log activity, monitor general usage patterns, and perform other activities that are necessary for the delivery and availability of service.

Receipt of a report or discovery of inappropriate or unauthorized use of computing and network resources may trigger monitoring and investigation by authorized FCT staff.

FCT systems owners and operators may specifically monitor the activity of individual users including files, session logs, content of communications, and Internet access without notice, when:

The user's activity prevents access to computing and network resources by others.

General usage patterns indicate that unacceptable activity is occurring.

There is reasonable cause to believe that a user has violated or is violating policy or law.

It appears necessary to do so to protect FCT from liability.

It is required by and consistent with law.

Evidence of misuse of computing resources will be referred to appropriate FCT officials. Evidence of possible criminal activity, which could include user files, email, and/or activity logs, will be turned over to appropriate FCT and law enforcement officials.

6.3. Electronic Data and Records Management

Much of the vast amount of electronic data generated throughout the college comprises official FCT records and requires specific management and handling practices and procedures as defined by FCT and state law.

All FCT system owners, operators, data custodians, and users are obligated to understand the nature of the data they generate, use, or store and to ensure that they are managing that data in full compliance with all state laws and FCT records management policies. All FCT system owners, operators, data custodians, and users are required to properly manage and protect electronic data they may be using, transmitting, and storing.

FERPA is the primary source for direction and information regarding personally identifiable information.

6.4. Access Controls

FCT has many different computing environments hosted on the institution networks, and within FCT departments and business units. These environments require different security measures. Consequently, access control measures required for establishing users' access to any FCT computing resources should be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved.

All system owners, operators, and data custodians are responsible for ensuring that their systems are properly protected with appropriate access control measures based on the criticality of their systems and the data involved.

In addition, all computing systems hosted on FCT networks must support and comply with the following fundamental access control measures, functions, and operating principles:

Systems are required to have an access control mechanism that allows for an appropriate level of authorization and allocation of system and data resources to individual users. Access mechanisms can be physical, transaction-based, role-based, time-based, user-based, or use any other reasonable control method appropriate for the systems' functions.

Shared systems are required to have the capability to log basic information about user access activity and to create historical logs and access violation reports.

System access accounts for users must be based on a unique identifier, and no shared account is allowed except as authorized by the system owner or operator and where appropriate accountability can be maintained.

Users' system access must be based on the principle of least privilege and the principle of separation of duties.

Computer applications must be developed and integrated in a way that maintains individual user accountability and audit capability.

Documented procedures should be in place for issuing, altering, and revoking access privileges on shared systems.

6.5. Systems and Network Security

In light of the complex and diverse nature of the different computing environments hosted on FCT networks and the wide range of statutory and regulatory compliance requirements, all systems and network security measures must be based upon the functional nature and degree of criticality of the computer systems, network resources, and data involved.

All system owners and operators are responsible for ensuring that they have implemented all necessary security measures. Failure to do so risks creating security breeches or other incidents and could lead to temporary restrictions or even suspension of access to FCT network resources.

1) Systems Security—Minimum Measures and Practices

To protect the availability and integrity of FCT computing resources, all computing systems and servers hosted on FCT networks should comply with the following systems security measures and practices:

Operating systems and applications must be maintained with the timely application of all related vender-issued patches necessary to prevent the systems from being compromised and/or causing disruptions of network services and/or other systems.

FCT-owned Networks must install antivirus software and maintain procedures for regular signature updates as per the FCT Anti-virus Policy.

Shared systems are required to have a technical access control mechanism that allows authorization and allocation of system and data resources to individual users.

Procedures must be maintained for regular backup of all data and system files necessary for discovery and recovery purposes. All backup media should be stored properly in a location authorized by the data owner with protections that allow access to the data by authorized personnel only. The ability to recover data from backups should be tested regularly.

Critical servers must be housed in protected areas such as server sanctuaries (locations where suitable physical and logical security measures can be implemented).

2) Network Security—Minimum Measures and Practices

To protect the security, availability, and integrity of FCT network resources, all computing systems and servers hosted on FCT networks should comply with the following security measures and practices:

Support proactive vulnerability probing and reporting by FCT authorized technicians to help manage system security needs.

Use secure protocols (e.g., SSL/SSH/Kerberos) for accessing all services that require authentication.

Report all security breaches to the appropriate security entity (CNS, and/or the FCT ISSO).

Display security-warning banners prior to allowing the access log-on process to be initiated on systems running applications that are accessible on the FCT-owned network. These security banners must inform all users that the system or application being accessed is proprietary, that it should be accessed only by authorized users, and that system use is monitored for enforcement purposes.

6.6. Physical Security

Physical security measures are an important part of any effort to protect information system assets and services. As with logical security measures at FCT, the physical security measures required for protecting FCT computing resources must be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved.

FCT has a wide spectrum of information systems deployments. They include:

Data center facilities.

Modest-sized server rooms.

Computer labs.

Telecommunications closets and vaults of all shapes and sizes.

Media storage areas.

Desktop computer workstations and printers.

Wireless and mobile systems.

These technology deployments require different physical security measures. These measures are especially important when sensitive information is involved. All system owners and operators are responsible for ensuring that they have implemented the appropriate physical security measures for their particular computing environment. All users are required to respect the physical security measures in place.

6.7. Personnel Security Measures

This section outlines security measures and procedures that should be established and maintained when working with FCT personnel throughout the employment process and when dealing with vendors, contractors, and temporary employees.

1) Measures for Hiring Employees

Comprehensive pre-employment screening is recommended for all potential candidates for key technical positions when those positions include an actual or potential wide span of systems control, and/or access to sensitive information, especially personally identifiable information or FCT financial information. This screening could include checking and confirming references, background checks for criminal convictions (both federal and local, as necessary), and reviewing educational records and credit reports. All hiring officials should consider using such screening practices when hiring for key technical positions, regardless of employee type (contract, classified, professional, academic, or temporary).

All pre-employment inquiries must be conducted in full compliance with state and federal laws.

All FCT departments and business units should have procedures in place to provide new employees with information about user responsibilities and guidelines associated with their assigned computer and network privileges and resources, including access to this document and related departmental policies, procedures, and guidelines. Appropriate supervision of new employee access to systems and data should be standard practice. New employees should be made aware that secure computing practices will be part of their performance reviews.

All physical and logical access to computing and network facilities and resources should be assigned in accordance with the principle of least privilege and principle of separation of duties.

2) Measures for Separating Employees

All FCT departments and business units should establish and maintain processes and procedures to properly and quickly close and remove all computing system and network privileges and resources when an employee is separated, even if the employee is going to another job within FCT. These processes and procedures should include the following:

The separated employee's immediate manager is responsible for notifying all system owners and operators, or the designated system administrator handling the computer or communications accounts, to close all related accounts and remove all access capabilities related to the separated employee.

Separated employees may not retain, give away, or remove from FCT premises any FCT information (electronic or hard copy) other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other FCT information in the custody of the departing employee must be turned over to the employee's immediate supervisor at the time of departure.

At the time of separation, all FCT property must be returned. This includes portable computers, printers, modems, software, cellular telephones, digital pagers, PDAs, documentation, building keys, lock combinations, physical keys, encryption keys, and access cards.

3) Measures for Employees on Leave or Suspension

All FCT departments and business units should establish and maintain processes and procedures to properly and quickly close and remove all computing system and network privileges and resources when an employee is suspended or is taking an extended leave of absence (including long-term illness or disability). It is important to use the same security measures for suspended employees as are used for separating employees. In addition, extended leaves of absence may require these measures, at the supervisor's discretion, taking into consideration such factors as level of access, nature and scope of computer applications and permissions, and duration of absence.

4) Measures for Vendors

Vendors with access to computers and networks should meet many of the same standards placed on employees. They should understand the security policies and practices. Their access should be limited to just what is necessary for them to meet their contract requirements. When appropriate, vendors should be escorted into physically restricted areas. When their job is complete, they should return all access devices, and their log-on privileges should be terminated.

6.8. Policy Enforcement

Individuals who violate this policy may be denied access to FCT resources and may be subject to other penalties and disciplinary action within and outside FCT. Departmental managers are expected to work with appropriate FCT resources in investigating and addressing suspected violation of this policy.

FCT may temporarily suspend, block, or restrict access to computing resources and accounts at any time when it reasonably appears necessary to do so in order to protect the integrity, security, or availability of FCT computing and network resources or to protect FCT from liability. FCT will refer suspected violations of applicable law to appropriate law enforcement agencies.

In general:

If violations of this policy are minor and unintentional, FCT will take appropriate actions to resolve the issue, and violators may be subject to disciplinary measures.

If violations of this policy are a result of negligent or deliberate acts, FCT will take appropriate actions to resolve the issue including disciplinary measures up to and including termination of employment or expulsion.

In addition to any other measures taken, if violations of this policy are a result of suspected illegal activities, FCT will notify appropriate college authorities and law enforcement agencies.

FCT reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of violations of this policy.

6.9. Policy Maintenance

This policy and the related guidelines will be reviewed yearly. A major security compliance audit must take place every three years.