Fairfield
UNIVERSITY

Information Technology Security Policy

004 Information Technology Security Policy

AUDIENCE:

The audience of this policy includes those involved with the implementation and management of information technology (IT).

PURPOSE:

The purpose of this policy is to ensure the protection of the University's information assets from accidental or intentional unauthorized access or damage while also preserving and nurturing the open, information-sharing requirements of its academic culture.

This policy establishes requirements to ensure the confidentiality, integrity, and availability of the information assets.

SCOPE AND APPLICABILITY

This policy governs and establishes Fairfield University’s requirements for information security protections as they apply to the University’s information and computing systems.

This Policy also governs the protection of information during electronic communication and data transmission processes both internal and external.

POLICY STATEMENT

Fairfield University Information Technology Services Department shall develop and implement the appropriate safeguards to ensure the protection of the University’s information assets.

004.1 ACCESS CONTROL

Access to assets and associated facilities shall be limited to authorized users, processes, or devices, and to authorized activities and transactions based on documented business need and in line with principle of least privilege access:

Identities and Credentials

- Identities and credentials shall be managed for authorized devices and users and all access shall be required to have passwords with industry accepted complexity settings appropriate for the risk of the systems or data;

- Newly created accounts shall be set to require users to change the provided password at first login;

- All access control credentials shall be approved prior to access being granted to any system or data;

- Staff shall have their accounts disabled upon transfer or termination;

    - Since there could be delays in reporting changes in user responsibilities, periodic user access reviews shall be conducted minimally every six months for systems containing restricted data by data custodians; as defined and required by the Asset Management Policy.

- All users shall have unique credentials;

- Identity verification shall be performed prior to resetting a password;

- Temporary or vendor accounts shall have expirations and be disabled upon completion of work;

- A custodian (usually a systems administrator or asset owner) for vendor accounts shall be identified and shall be responsible for access control of the account;

- Accounts used by vendors for remote maintenance (including remote access accounts) shall be enabled only during the time period needed where appropriate;

- Secrets such as service account credentials or API keys shall be securely managed based on Data Access Governance Policy;

- Official Fairfield University social media accounts shall only be established with authorization from marketing and communications, use Fairfield University email addresses and utilize the strongest available account protection mechanisms provided by the vendor including multi-factor authentication (MFA) where applicable;

- Information systems shall be automatically password protected (locked), or auto log off sessions after a defined period of time, following industry best practices; and

- Network access control mechanisms shall be maintained to ensure only approved devices connect to the University’s network.

Physical Access

- Physical access to assets shall be managed and protected;

- Access to all data centers shall be limited to authorized personnel;

- Video monitoring of access shall be placed at all entrances of data centers;

- All access to communications distribution locations (wiring closets) shall be limited to authorized personnel;

- All visitors accessing data centers or communications distributions locations shall be logged or escorted;

Remote Access

- Remote access shall be managed by the Information Technology department;

- Firewalls and other technology shall be used to restrict remote access to only approved remote access mechanisms;

- Remote access must be strictly controlled by the use of unique user credentials, including a username and password;

- Remote access passwords shall be granted only to the individual to whom they were assigned and may not to be shared;

- All hosts that are connected to Fairfield University internal networks via remote access technologies (such as VPN) must have up-to-date anti-virus software implemented, and current operating system security patches installed ;

- Organizations or individuals who wish to implement non-standard Remote Access solutions to the Fairfield University network must obtain prior approval by the Office of Information Security;

- A mobile device management system shall be maintained for University owned and ‘bring you own devices’ that access University systems; such a system is responsible for ensuring that university data is protected based on regulatory and legal obligation.

- Remote access mechanisms must include the following technical capabilities:
    - Allow only identified, authenticated, and authorized users to connect;
    - A Multi Factor Authentication mechanism;
    - Provide for strong encryption of traffic;
    - Audit logs contain sufficient information to establish the following:
        - Event type (authentication, connection, or disconnection);
        - Date and time;
        - User associated with the event;

  - Remote and local IP addresses;
  - Event success or failure;

- Interconnections to Fairfield University's network (i.e. Point-to-Point VPN) shall require interconnection agreements. Access must be restricted to the minimum necessary to achieve the goals of the interconnection.

Least Privileged Access

- Access permissions shall be managed, incorporating the principles of least privilege and separation of duties;

- Access to critical systems or sensitive data will only be provided to users based on business requirements, job function, responsibilities, or need-to-know;

- All additions, changes, and deletions to individual system access must be approved by the appropriate supervisor with a valid business justification;

- On a bi-annual basis, University data custodians will audit all user and administrative access to critical systems or sensitive data. Discrepancies in access will be remediated accordingly;

- Data Custodians with privileged access to Restricted data shall have two user IDs: one for normal day-to-day activities or and one for performing administrator duties;

- Privileged access may only be used to perform administrator functions;

- Administrators may not use their privileged access for unauthorized viewing, modification, copying, or destruction of system or user data;

- Local computer accounts should only be used when managing systems while physically present (standing at the keyboard). In all other cases designated privileged accounts shall be used;

- Authentication to systems with a privileged account shall only be authorized when completed with multifactor authentication (MFA);

- Users with privileged access must protect the confidentiality of any information they encounter while performing their duties; and shall be responsible for complying with all applicable laws, regulations, policies, and procedures;

- Users shall formally request privileged access; all normal user ID and password policies and procedures apply; and

- The Office of Information Security shall maintain an inventory of approved active privileged accounts.

004.2 DATA SECURITY

Information and records (data) shall be protected consistent with Fairfield's risk strategy to protect the confidentiality, integrity, and availability of information.

Data-at-rest

- Data-at-rest shall be protected;

- Endpoints (such as a desktop or laptop computers) shall be encrypted to preserve the confidentiality and integrity of University data classified as Restricted or Private.

Data-in-transit

- Data in transit shall be encrypted with industry accepted encryption mechanisms in accordance with its sensitivity.

Capacity and Availability

- All systems shall be monitored to ensure availability is maintained according to their criticality classification; and

- All systems shall maintain reserve capacity to ensure availability according to their criticality classification as outlined in the Asset Management Policy.

Data Leaks

- Protections against data leaks shall be implemented when applicable;

- Systems shall be maintained to protect Restricted and Private University data from leaving authorized networks and systems as outlined in the Minimum Security Standard;

- Email protection systems shall be maintained to protect against email based attacks (phishing, spam, etc.);
- The University shall maintain anti-malware on all system considered susceptible to malware infection. These systems shall be implemented with industry accepted best practices.

Integrity Checking

- Integrity checking mechanisms shall be enabled and used to verify software, firmware, and information integrity.

Development Environment

- The development and testing environment(s) shall be separate from the production environment and based on the Fairfield University Application Security Standard.

004.3 INFORMATION PROTECTION PROCESSES AND PROCEDURES

Security policies that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities, processes, and procedures shall be maintained and used to manage protection of information systems and assets.

Baseline Configurations

- A baseline configuration standard of information technology systems shall be created and maintained by data custodians and approved by the Office of Information Security;
- This includes but is not limited to:
  - End user system images
  - Server system virtual machine templates
  - Network switches
  - Standard cloud configuration
  - Firewalls
  - Database servers

System Development Life Cycle

- A System Development Life Cycle (SDLC) to manage all development projects is implemented; and
- All SDLC shall include:
  - Auditable version and change control
  - Peer review
  - 100% Code Execution
  - Separation of Duties for all code production deployment

Change Control

- Configuration change control processes shall be in place; and

- Change control shall document, approve, and validate all changes to the University's computing environment.

Backups

- Backups of information shall be conducted, maintained, and tested periodically; and
- Backups shall be encrypted.

Human Resources

- Cybersecurity shall be included in human resources practices (e.g., de-provisioning termination notifications, personnel screening, onboarding training).

Vulnerability Management

- A vulnerability management standard shall be developed and implemented; and
- Vulnerabilities shall be identified, documented, remediated, and verified according the vulnerability management standard.

004.4 MAINTENANCE

Maintenance and repairs of information system components shall be performed consistently.

Maintenance

- Maintenance and repair of organizational assets shall be performed and logged in a timely manner, with approved and controlled tools; and
- Software maintenance (updates, upgrades, security patches) shall be implemented in accordance with the risk profile of the system and the University's patch management standards.

Remote Maintenance

- Remote maintenance of organizational assets shall be approved, logged, and performed in a manner which prevents unauthorized access.

004.5 PROTECTIVE TECHOLOGY

Technical security solutions shall be managed to ensure the security and resilience of systems and assets.

Audit / Logging

- Audit/log records shall be determined, documented, implemented, and reviewed; and

- The Office of Information Security shall monitor and investigate suspicious/malicious activity from Intrusion Prevention Systems (IPS), anti-virus system, or other security systems.

Wireless Networks

- Access to the wireless service shall be restricted to current students, faculty, staff, and guests whom have been authorized;

- Users accessing non-public University data shall be authenticated to wireless networks; and

- The wireless service shall protect authentication credentials and data through the use of industry accepted encryption.

Communications and Control Network

- Communications and control networks shall be protected;

- The University shall monitor and control communications at the external network boundary and at key internal boundaries within the University;

- The University shall maintain a network firewall standard which shall document traffic flow between network segments;

- The University shall implement network boundary controls to segment areas of the network containing different classifications of data and document such boundaries and configurations within the Fairfield University network firewall standard;

- The University shall implement a policy of least privilege concerning network access control such that traffic is denied by default and allowed only by documented exception;

- The University shall monitor, detect, and deny outgoing communications traffic posing a threat to external information systems and audit the identity of internal users associated with denied communications;

- The organization shall protect against unauthorized physical network connections. By implementing a network access control standard to document the process of gaining authorization to the Fairfield university network and denying unauthorized methods;

- Boundary protection devices (firewalls) shall fail securely in the event of an operational failure.

ROLES AND RESPONSIBILITIES:

Job titles and business offices directly involved in the practices related to the policy:

a) Chief Information Security Officer

b) Information Technology Services

DEFINITIONS:

Information assets: Include University data, and information systems,(Such as computers, network connected devices)and documents regardless of their medium and regardless of their location.

University's information: Is considered all information or data generated or acquired, in printed or digital form, by Fairfield students, faculty, staff or others who make use of Fairfield's information technology resources and services.

ENFORCEMENT:

Personnel using Fairfield University information resources in opposition to this policy may be subject to limitations on the use of these resources, suspension of privileges (including internet access), as well as disciplinary and/or legal action, including termination of employment.

REVISION HISTORY:

Date	Author	Comment
02/23/2018		Original Version

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version