FIU Acceptable Use of IT Resources Policy

Purpose

The purpose of the FIU Acceptable Use of IT Resources Policy is to establish acceptable practices regarding the use of FIU Information Resources in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Scope

The FIU Acceptable Use of IT Resources Policy applies to all faculty, staff, and students and authorized third party affiliates (consultants, vendors, persons of interest). Any exceptions to this standard must be approved by the Information Technology Security Office at security@fiu.edu.

Policy

Acceptable Use

- Users are responsible for complying with FIU policies when using FIU information resources. If requirements or responsibilities are unclear, please seek assistance from the Information Security Team.
- Users must promptly report harmful events or policy violations involving FIU assets or information to the Information Technology Security Office (ITSO) at security@fiu.edu. Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to FIU resources.
    - Data incident: any potential loss, theft, or compromise of FIU information.
    - Unauthorized access incident: any potential unauthorized access to an FIU Information Resource.
    - Facility security incident: any damage or potentially unauthorized access to an FIU owned, leased, or managed facility.
    - Policy violation: any potential violation to this or other FIU policies, standards, or procedures.
- Users should not purposely engage in activity that may
    - harass, threaten, impersonate, or abuse others;
    - degrade the performance of FIU Information Resources;
    - deprive authorized FIU users access to a FIU Information Resource;
    - obtain additional resources beyond those allocated;
    - circumvent FIU computer security measures.
- Users should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, FIU users should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any FIU Information Resource.
- Single sign-on, two-factor authentication, and encryption should be used at all times, whenever available.
- FIUInformation Resources are provided to facilitate university business and should not be used for personal financial gain.
- Users are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using FIU Information Resources.

- Users should not intentionally access, create, store or transmit material which FIU may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a least privilege model and only granted if needed.
- Users are permitted to use only those network and host addresses issued to them by FIU DoIT and should not attempt to access any data or programs contained on FIU systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal FIU networks and/or environments must be made through approved, and FIU-provided, virtual private networks (VPNs).
- Users should not divulge any access information to anyone not specifically authorized to receive such information, including IT support users.
- Users must not share their personal authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Multi-factor authentication information
    - Access cards and/or keys,
    - Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Access cards, security tokens, and/or keys that are no longer required must be returned to physical security.
- Lost or stolen access cards, security tokens, and/or keys must be reported to physical security users as soon as possible.

Internet

- Use of the Internet with FIU networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
    - Recreational games,
    - Streaming media,
    - Personal social media,
    - Accessing or distributing pornographic or sexually oriented materials,
    - Attempting or making unauthorized entry to any network accessible device, on any networking including FIU
    - Violation of any FIU policy and state, local, or federal laws.
- Access to the Internet from outside the FIU network using a FIU owned computer must adhere to all of the same policies that apply to use from within FIU facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- Use of personally owned devices must be in compliance with all other FIU policies.
- All FIU owned mobile devices must maintain up-to-date versions of all software and applications.
- All users are expected to use mobile devices in an ethical manner.
- Theft or loss of any mobile device that has been used to create, store, or access confidential or internal information must be reported to the FIU Security Team immediately.
- FIU IT Management may choose to execute “remote wipe” capabilities for mobile devices without warning
- In the event that there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the user’s possession as part of a formal investigation.
- All mobile device usage in relation to FIU Information Resources may be monitored, at the discretion of the Information Technology Security Office.
- Jail-broken or rooted devices should not be used to connect to FIU Information Resources.

- Level 3 - Confidential information should only be stored on devices that are encrypted in compliance with the FIU Configuration Management Plan . Contact the ITSO for more information.
- Level 3 - Confidential information should not be stored on any personally owned mobile device.
- FIU IT support for personally owned mobile devices is limited to assistance in complying with this policy. FIU IT support may not assist in troubleshooting device usability issues.

Physical Security

- Photographic, video, audio, or other recording equipment, such as cameras and cameras in mobile devices, is not allowed in secure areas.
- Users must display photo ID access card at all times while in secured buildings.
- Users must badge in to access-controlled areas. Piggy-backing, tailgating, door propping and any other activity to circumvent door access controls are prohibited.
- Visitors accessing card-controlled areas of facilities must be accompanied by authorized users at all times.
    - Eating or drinking are not allowed in data centers. Caution must be used when eating or drinking near workstations or information processing facilities.
    - Maintain access to secured/locked locations updated at all times.

Privacy

- Information created, sent, received, or stored on FIU Information Resources are not private and may be accessed by FIU DoIT employees at any time, under the direction of FIU executive management and/or Human Resources, without knowledge of the user or resource owner.
- FIU may log, review, and otherwise utilize any information stored on or passing through its Information Resource systems.
- Systems Administrators, FIU IT, and other authorized FIU users may have privileges that extend beyond those granted to standard business users. Users with extended privileges should not access files and/or other information that is not specifically required to carry out an employment related task.

Security Training and Awareness

- All new users must complete an approved security awareness training class prior to, or at least within 90 days of hire, or access to FIU Information Resources may be restricted.
- All users must be provided with and acknowledge they have received and agree to adhere to the FIU Information Security Policies before they are granted to access to FIU Information Resources.
- All users must complete the security awareness training annually.

Social Media

- Communications made with respect to social media should be made in compliance with all applicable FIU policies.
- Users are personally responsible for the content they publish online.
- Creating any public social media account intended to represent FIU, including accounts that could reasonably be assumed to be an official FIU account, requires the permission of FIU External Relations.
- When discussing FIU or FIU -related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an FIU representative, and
    - Make it clear that you are speaking for yourself and not on behalf of FIU, unless you have been explicitly approved to do so.
- Users should not misrepresent their role at FIU.

- When publishing FIU-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; "The opinions and content are my own and do not necessarily represent FIU's position or opinion."
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with FIU will not be tolerated.
- Level 3 - Confidential data, ad defined in the Data Classification Standard, may not be published online in any form.
- Users approved to post, review, or approve content on FIU social media sites must follow the FIU Social Media Used to Disseminate University Content Policy.

Voicemail

- Users should not access another user's voicemail account unless it has been explicitly authorized.
- Users must not disclose Level 3 - Confidential data in voicemail messages.

Incidental Use

- As a convenience to FIU users, incidental use of Information Resources is permitted. The following restrictions apply:
  - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to FIU approved users; it does not extend to family members or other acquaintances.
  - Incidental use should not result in direct costs to FIU.
  - Incidental use should not interfere with the normal performance of an employee's work duties.
  - No files or documents may be sent or received that may cause legal action against, or embarrassment to, FIU or its customers.
- Storage of personal email messages, voice messages, files and documents within FIU Information Resources must be nominal
- All information located on FIU Information Resources are owned by FIU may be subject to open records requests and may be accessed in accordance with this policy.

Definitions

See Cybersecurity Glossary

Resources

- AI Acceptable Use Guideline
- Data Classification Standard
- Data Stewardship Policy
- FIU Approved Services
- Incident Response Plan
- IT Asset and Computer Purchasing Policy
- Media Sanitization
- Social Media Used to Disseminate University Content Policy

Enforcement

Each member of the University community is responsible for adhering to all federal, state and local laws and FIU rules, regulations and policies, as the same may be amended from time to time, pertaining to the security and protection of electronic information resources that he/she uses, and/or over which he/she has access or control.

Persons who fail to adhere to this Policy may be subject to penalties as provided by law and/or disciplinary action, including dismissal or expulsion. Violations will be handled through the University disciplinary policies applicable to employees and students. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Unauthorized or fraudulent use of university computing or telecommunications resources can also result in felony prosecution as provided for in the Federal and State of Florida Statutes

Version History

Initial Effective Date: May 4, 2002
Review Dates (review performed, no updates): n/a
Revision Dates (updates made to document): June 4, 2026