Advancement | UCF Foundation, Inc.

Information Security Policy

Policy# 10.10
Effective Date: 09/09/2020
Responsible Department: Information Technology Services

1. PURPOSE

The purpose and objective of this information security policy is to protect University of Central Florida Foundation (Foundation) systems, data and information assets from all threats, whether internal or external, deliberate or accidental.

2. APPLICABILITY

This policy applies to full, part-time and temporary University of Central Florida (University) and the Foundation employees, contractors, consultants, interns, students, and other workers at the Foundation, including all personnel affiliated with third party employees, who use the Foundation's information technologies and resources. This policy also applies to all Foundation systems, data, or information assets.

Users shall use University and the Foundation's Electronic Information Resources responsibly in accordance with this policy and the University policy for 4-007.1 Security of Mobile Computing, Data Storage, and Communication Devices

3. POLICY

This policy is designed to be the overarching information security policy for the Foundation and is the primary policy under which all other security standards reside. It is to ensure that the Foundation will comply with all relevant internal information technology controls and regulatory requirements in respect to information security. The policy will describe specific Foundation rules on information security and reference any subservient policies and/or standards that will describe policy in more detail.

Authentication
Before granting access to system resources, all Foundation' systems will require authentication of users or computer jobs requesting access.

Access Control
Protection of Foundation data and software is partly achieved via access control mechanisms; system resources will be restricted to specifically authorized users.

Software Control
Software modifications developed by or for the Foundation will be controlled throughout the process using programming techniques and procedures designed to ensure security, integrity and reliability of the end product to include: software application changes or enhancements, including enhancements to the core business applications such as Blackbaud CRM and Financial Edge; software upgrades, including patches

and bug fixes; and data extraction for reporting purposes.

Antivirus
Current antivirus protection will be maintained on all servers, desktop computers, and laptop computers.

Encryption
Encryption processes must not be used for Foundation information unless the processes are approved by the Director for Advancement Information Technology Services. In some jurisdictions, encryption is illegal, or the key may need to be disclosed to government agencies. To ensure that users are not inadvertently breaking the law, Foundation ITS and the Director for Advancement Information Technology Services will be involved in decisions to use encryption.

To protect Foundation informational assets contained on mobile devices in the event of loss or theft, laptop computers are to have all data encrypted through an approved method.

Network Security
All employee network devices are to be controlled and maintained by the University's Information Technology Department (UCF IT). The Foundation's Information Technology Department (Foundation ITS) will coordinate with UCF IT to coordinate all necessary changes to the network switches. All network changes will follow standard change control procedures. All network augmentations, including hardware and software, will be authorized by UCF IT.

System Configuration
Services and applications that will not be used must be disabled where practical. UCF IT will implement platform specific hardening to ensure security where applicable. UCF IT will ensure that internal and external hosted servers comply with Foundation ITS and UCF IT security policy and server configuration standards. Foundation ITS will ensure that desktops and laptops comply with Foundation and University security policy and configuration standards. Only Foundation ITS and UCF IT may deploy and manage servers, desktops and laptops. Foundation users are not permitted to install or implement any software that would be considered a server product.

Administrator accounts are limited to Foundation ITS personnel and must be approved by the Director for Advancement Information Technology Services. Exceptions to this rule will require a valid business requirement.

Third Parties, Vendors, and Cloud Services
For any third party or vendor system that may have access to, store, transmit, process, or collect any Foundation data on our behalf, the Foundation will engage the University's Information Security Office for a formal review of the third party or vendor system through their Vendor Risk Management (VRM) process before any substantial Foundation data is transmitted to said third party or vendor system.

Furthermore, the Foundation shall strive to adhere to the standards delineated in the University's Security Standard 120 VRM Standards.

Contractors and consultants will be granted access to Foundation systems on an as-needed basis after all appropriate University, Foundation HR, and Foundation ITS paperwork has been completed and signed.

4. CLARIFICATION

Requests for clarification of this policy should be sent to the Associate Vice President for Advancement, Strategy and Chief Operating Officer.

Certified as approved by the Executive Committee of the Foundation Board of Directors on September 9, 2020.

Michael Morsberger Digitally signed by Michael Morsberger Date: 2020.11.18 10:03:53 -05'00'

Name: Michael J. Morsberger
Title: Vice President for Advancement and Chief Executive Officer

Revision history:
Adoption Date: March 5, 2013
Revised: August 27, 2020

History: 752