Information Security

Security Standards

University Advancement follows information security standards set by VCU Technology Services and the Commonwealth of Virginia (VITA). More specifically, the guidelines specified below should be adhered to:

- Confidential business, research and supporting data must be protected by strong passwords and be stored on VCU Technology Services supported servers.
- Data provided by Advancement Services will be sent to VCU staff by the most secure method available. Data will only be supplied to secure sites if required by an external vendor contracted for services to VCU.
- All PC's supported by Advancement Services will adhere to best practices for physical security, firewalls, patching, strong passwords and virus protection
- No data will be stored on any non-network device or media except for backup media, unless the data is encrypted and there is a written exception approved by the VCU CIO (for form and procedures, see VCU Security Standard for Encryption http://infosecurity.vcu.edu/)

	SECURITY STANDARDS CHECKLIST **The following provides a checklist for adherence to VCU Information Security Standards**
Workstation Requirements	• Complex Passwords (8-16 characters, Upper/Lower, Numerical or Special character) • VCU approved antivirus system • Automatic lock of workstation after 10 minutes of inactivity. • Disable unneeded local accounts • Automatic Updates to be enabled (daily check) and Windows Firewall enabled; only VCU supported PC Operating Systems with most current patch installed • Maintain current patch level for all desktop/supported applications • The "remember passwords feature" in applications (e.g. web browsers) must not be used.
Physical Security Requirements	• Office doors and computers must be locked when an user is away from the desk • Passwords must not be written and stored in areas without physical protection. (e.g. sticky notes on monitor or keyboard) • Documents containing sensitive information should be delivered only to the lockbox located at the Blanton House and once received must be stored in a physically secure location (behind locked door, locked drawer, in safe). According to Records Management Standards and VCU Document Destruction Services, documents with sensitive or confidential information which are no longer needed are disposed in the secured recycling bin.
Data Protection	• All business data must be stored on the network servers • Transfer of files (internal to VCU) containing sensitive data must be encrypted or protected and deleted/destroyed when no longer needed. • Data supplied to external vendors must be sent to a secured site (https)
Remote Access	• All remote access into the VCU Network must use VCU approved tools (WebVPN, F5, Cisco VPN
Communication/ Security	• Passwords must not be electronically stored, sent or received in clear text • Encryption is required when sensitive data is accessed

Data Breach Notification	• Lost or stolen computers and electronic storage media must be reported to the VCU ISO and Police within **24 hours** • Unauthorized access of sensitive information must be reported to Advancement Services-Information Technology within **24 hours**