Standards	Statement	Restricted	Sensitive	Internal
General				
Access Control	Anyone accessing, or having access to data, has passed a background check as defined by the university. This includes faculty, students, staff, student workers, and affiliates.	Mandatory	Mandatory	Mandatory
Data Handling	Paper documents are protected and shredded when discarded. Employees do not discuss or share data outside of the workplace or with anyone who does not have a specific "need to know".	Mandatory	Mandatory	Mandatory
Public Access to data	Employees utilize university approved VPN to send or receive NJIT data when using public Wi-Fi networks.	Mandatory	Mandatory	Mandatory
Role-based Access Control/Least privilege principle	An individual should have only the minimum access privileges necessary to perform a specific job or task and nothing more.	Mandatory	Mandatory	Mandatory
Account deprovision	Separated employees and affiliates shall lose all employee/affiliate level access as of their separation date unless it is necessary to remove access prior to separation date or within 24 hours of seperation	Mandatory	Mandatory	Mandatory
Endpoint Devices				
Anti-virus & Malware Protection	Computers have antivirus software installed. Crowdstrike is available for all NJIT owned computers (Windows, Mac, and Linux). Windows Defender is available for personaly owned Windows computers.	Mandatory	Mandatory	Recommended
Physical Security	Faculty and staff are responsible for storing their computing devices in a secure area. Computing devices are configured to utilize a display lockout.	Mandatory	Mandatory	Mandatory
Security logging	User access, login information, and secruiry logs are maintained.	Mandatory	Mandatory	Mandatory
Multi-factor Authentication (MFA)	Multi factor authentication is enabled.	Mandatory	Mandatory	Mandatory
Data Sanitization	University owned equipment, removed for off-site maintenance or retirement, is sanitized of data.	Mandatory	Mandatory	Mandatory
Patching Management	Security patches are applied as outlined in NJIT's Patch Managment Policy.	Mandatory	Mandatory	Mandatory
Servers				
Security Management Software	Security and management software is installed.	Mandatory	Mandatory	Mandatory
Backups	Data is regularly backed up to maintain data integrity and availability.	Mandatory	Mandatory	Mandatory

Access Review	Access control and password policies are applied and privledged access is reviewed quarterly.	Mandatory	Mandatory	Mandatory
Session Control	Session timeouts are enabled.	Mandatory	Mandatory	Recommended
Multi-factor Authentication (MFA)	Multi factor authentication is enabled.	Mandatory	Mandatory	Mandatory
Physical Security Controls	IT equipment, including servers and data storage devices, are kept within secure areas protected by physical and environmental controls.	Mandatory	Mandatory	Mandatory
Remote Access Controls	VPN is required for off-campus access	Mandatory	Mandatory	Mandatory
Security Logging	User access and login information is maintained. Security logs are enabled to maintain a complete, tamper-proof audit trail of all processes initiated by the system and are forwarded to the Splunk central log aggregation/management system.	Mandatory	Mandatory	Mandatory
Vulnerability Scanning and Patching	Scans of university owned systems are completed quarterly, results of scans must be shared and vulnerabilities remediated upon within 90 days.	Mandatory	Mandatory	Recommended
Data Sanitization	University owned equipment, removed for off-site maintenance or retirement, is sanitized of data.	Mandatory	Mandatory	Mandatory
Patching Management	Security patches are applied as outlined in NJIT's Patch Managment Policy.	Mandatory	Mandatory	Mandatory
Security, Privacy, and Legal Review	Data stewards informs Data Owners to follow best practices based Data Risk Assessment process and implement recommendations prior to deployment.	Mandatory	Mandatory	Mandatory
Applications & Cloud-Based Services				
Session Controls	Application session timeout is enabled.	Mandatory	Mandatory	Mandatory
Backups	Data is regularly backed up to maintain data integrity and availability.	Mandatory	Mandatory	Mandatory
Multi-factor Authentication (MFA)	Multi factor authentication is enabled.	Mandatory	Mandatory	Mandatory
Access Review	Access control and password policies are applied and privledged access is reviewed regularly.	Mandatory	Mandatory	Mandatory
Role Based Access Controls (RBAC)	Employ separation of duties for high-risk business functions is deployed across multiple users/roles.	Mandatory	Mandatory	Recommended
Security Logging	User access and login information is maintained. Security logs are enabled to maintain a complete, tamper-proof audit trail of all processes initiated by the system as defined by service operator.	Mandatory	Mandatory	Mandatory
Encryption	Data must be encrypted when in transit, both inside and outside of the university network. Data at rest, outside of an enterprise supported university system, is encrypted.	Mandatory	Mandatory	Recommended

Security Assessment	Security Assessment is performed before application and services including 3rd party products and services deployed. Security review of all the code, programs and updates before the production deployment	Mandatory	Mandatory	Recommended