Information Integrity and Availability Guide

Classification	Sensitive		Non Sensitive
	Confidential	**Proprietary-Internal Only**	**Public**
	Sensitive personal and/or University information for which unauthorized access may result in an invasion of privacy, identity theft, University liability or materially negative impact on the finances, operations, or reputation of the University. Examples include: information protected under HIPAA, FERPA, PCI, GLB, Export Controls, legally privileged information, personally identifying information (accounts, social security numbers, etc.) pending patent or University planning information, user passwords.	Information that is less sensitive than Confidential information, but that, if exposed to unauthorized parties, may have an adverse impact on the finances, operations, or reputation of the University. Examples include internal memos meant for limited circulation, draft documents or comments prior to public release. All University data is considered "Proprietary" unless otherwise documented.	Information that is generally available to the public, or that, if it was to become available to the public, would have no material adverse effect upon the finances, operations, or reputation of the University.
Integrity	**High**	**Medium**	**Low**
Electronic:	**Storage:** Secured servers, computing devices or databases **Controls:** Strong access controls, authentication and file protection mechanisms (IDS, anti-virus). Utilize approved encryption. Audit and event logging and monitoring. Access approval and periodic review required. Segregation of duties, SDLC, Change Management, secure coding. May require multifactor authentication and network isolation.	**Storage:** Secured **Controls:** Access controls, authentication, approvals or RBAC (role based) access and file protection mechanisms (IDS, antivirus). Mobile devices must utilize approved encryption. Moderate audit logging and monitoring. Segregation of duties, SDLC, Change Management, secure coding.	**Storage:** General Storage **Controls:** Anti-virus and general protection mechanisms and monitor-ing. Limited or no access controls, authentication or University access restrictions
Hardcopy:	**Storage and Controls:** Secure in locked cabinet or location with appropriate physical controls. Copies retained in secure off-site storage. Access restricted and approved.	**Storage and Controls:** Secured, recommend locked storage when not in use.	**Storage and Controls:** General storage when not in use. No restrictions.
Availability	**High – 24x7, Redundancy**	**Medium – 12x5, Tape or HA**	**Low**
Electronic:	Service Level Agreement with custodian, Change Management Controls, , Cross training of support personnel, Monitoring, Patch Management, Anti-virus, Backup, High availability-redundancy and recoverability off-site	Service Level Agreement with custodian, Change Management controls, Cross training of support personnel, Monitoring, Patch Management, Anti-virus, Backup, Tape or HA recovery and recoverability off-site.	Change Management controls, monitoring, Patch Mgt., Anti-virus, Backup, Best effort or not recoverable off-site
Hardcopy:	Copy stored off-site	Recommended copy stored off-site	No restrictions.