

<sup>[1]</sup> Safeguards: System = Information Technology, Admin = Administrative Procedures & Guidelines, Physical = Physical/Environmental security safeguards.

<sup>[2]</sup> Safeguard Guidelines by Data Category: M = Mandatory safeguard, R = Recommended, S = Suggested

<sup>[3]</sup> Measures: Procedures, processes and/or mechanisms to meet Internal Controls

**Any deviation from mandatory requirements must be documented and covered by adequate compensating control(s). The department of Internal Auditing is available to assist in reviewing compensating controls.**

Safeguards <sup>[1]</sup>			Category of Data <sup>[2]</sup>				Item Ref.	Measures <sup>[3]</sup>	Internal Control	Reference
System	Admin	Physical	I	II	III	IV				
<b>1 - Control Physical access to data</b>										
		X		R	M	M	1-1	e.g. Security alarms, card readers, locks, etc...	Institute physical security controls for each computer room, data center and other physical areas with systems that process and store data.	ICG XXVIII
		X				M	1-2	Video cameras with active 24/7 monitoring in Operating Centers	Constant monitoring is in place using video cameras in data centers to monitor storing/processing sensitive data. (Note: This is not mandatory for paper process and storage areas whose access is physically supervised or restricted when unmanned.)	CISP 12.1
	X	X		R	M	M	1-3		Consoles for systems that store and/or transmit sensitive data are "locked" to prevent unauthorized use. (Note: this refers to cabinet mounted servers with doors)	CISP 12.1
X	X	X	M	M	M	M	1-4	Physical disconnection of unused jacks, connection access authentication, etc.	Active GT Network jacks are only accessible to authorized users.	ISO -17799
		X	M	M	M	M	1-5		Network Access closets should be maintained locked with access only to authorized personnel.	
	X				R	M	1-6		Procedures must exist so all personnel can easily distinguish between employees and visitors, especially in areas where sensitive information is accessible.	
	X	X			R	M	1-7		ID badges: Visitor ID badges do not permit unescorted access to physical areas that store sensitive data.	CISP 12.3
	X	X			R	M	1-8		1. ID badges clearly distinguish employees from visitors/outside	
	X	X			R	M	1-9		2. Visitor badges contain a fixed expiration date.	
	X				R	M	1-10		3. Visitors are asked to surrender their ID badge upon departure or upon the expiration date.	
	X	X			R	M	1-11		Log all physical access. Retain this log for a minimum of three months.	
X	X	X			M	M	1-12		Physically secure all paper and electronic media.	
	X				R	M	1-13	e.g. Back up media is sent via secured courier or other traceable delivery mechanism.	Maintain strict control over the internal or external distribution of any kind of media.	
	X				R	M	1-14		Management approves transfers of all media that is moved from a secured area (especially when media is distributed to individuals).	
	X	X			R	M	1-15		Label the media as to data category.	
X	X		S	R	M	M	1-16		Maintain inventory of media and make sure it is properly stored.	
	X		S	R	M	M	1-17		Implement data destruction procedures.	

Safeguards <sup>[1]</sup>			Category of Data <sup>[2]</sup>				Item Ref.	Measures <sup>[3]</sup>	Internal Control	Reference
System	Admin	Physical	I	II	III	IV				
	X		S	R	M	M	1-18		1. Destroy media containing information when it is no longer needed for business or legal reasons	
	X		S	R	M	M	1-19		2. Shred or incinerate hardcopy materials when they have surpassed their retention date, or are no longer required.	
X	X		S	R	M	M	1-20		3. Purge, degauss, shred, or otherwise destroy electronic media so that data cannot be reconstructed.	
X	X				M	M	1-21	e.g. key issue logs, card issue logs, etc.	Fully document all physical access controls and procedures.	ICG XXVIII
<b>2 - Implement and maintain an information security policy</b>										
									Establish and publish a security policy that:	
	X		M	M	M	M	21		1. Addresses regulatory requirements.	FERPA, GLBA, HIPAA, BOR
	X		M	M	M	M	2-2		2. Reflects the unit's business objectives and addresses risk control standards, such as <i>segregation of duties</i> and other best practices.	
	X		S	R	M	M	2-3		3. Clearly define information security/stewardship responsibilities for all students, faculty, staff and contractors.	
	X		S	R	M	M	2-4		Develop operational security procedures that are consistent with the level of sensitive data processed/maintained	
									Assign to a qualified individual the following information security management responsibilities:	
	X		M	M	M	M	2-5		1. Establish, document, and distribute security policies and procedures.	
X	X		M	M	M	M	2-6		2. Monitor and analyze security alerts and information and distribute to appropriate personnel.	
X	X		M	M	M	M	2-7		3. Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	
X	X		M	M	M	M	2-8		4. Monitor and audit user account and authentication management, including additions, deletions, and modifications resulting from user changes and terminations.	
X	X				R	M	2-9		5. Monitoring and control over all access to data within the unit.	
	X		M	M	M	M	2-10		Make all authorized users aware of the importance of information security.	
	X		M	M	M	M	2-11		Require authorized users to acknowledge in writing on an annual basis that they have read applicable security policy(ies) and procedures.	
	X				S	M	2-12		Conduct background checks on all potential employees handling sensitive data to minimize the risk of attacks from internal sources.	
	X			S	M	M	2-13		Contractually require all associated third parties with access to Institute data to adhere to data security requirements. At a minimum, the agreement should address:	
						M	2-14		1. Security provisions outlined in ISO 17799, and any fines and penalties as specified by regulatory agencies for a lack of compliance with those provisions.	

Safeguards <sup>[1]</sup>			Category of Data <sup>[2]</sup>				Item Ref.	Measures <sup>[3]</sup>	Internal Control	Reference
System	Admin	Physical	I	II	III	IV				
			M	M	M	M	2-15		2. Business continuity in the event of a major disruption, disaster or failure.	
	X			S	M	M	2-16		3. Third party termination clauses to address compliance with security of information during contract terminations and related data transfers.	
			M	M	M	M	2-17		Vulnerability scans of the campus Administrative, Academic, and Research networks shall be performed every 30 days, and external network vulnerability scans semi-annually.	
<b>3 - Install and maintain a working firewall to protect data</b>										
				S	M	M	3-1		A firewall will be installed (hardware or software)	
X					S	M	3-2		Firewall at each internet connection and between DMZ and the Intranet	
			M	M	M	M	3-3		For any implemented firewall, a management plan exists that includes:	Visa CISP
X			M	M	M	M	3-4		1. Description of groups, roles, and responsibilities for logical management of firewall network components	
X			M	M	M	M	3-5		2. A documented list of services / ports necessary for the business	ISO -17799
	X		R	R	R	M	3-6		3. Justification and documentation for any available access protocols besides HTTP, SSL, SSH, and VPN used outside the firewall.	
X	X		M	M	M	M	3-7		4. Periodic review of firewall/router rule sets	
X	X		M	M	M	M	3-8		5. Management approval for external network connections and all other changes to the firewall configuration	
			M	M	M	M	3-9		6. Configuration standards for firewalls and routers, including testing of all changes prior to implementation.	
<b>4 - Keep Security Patches Up to date</b>										
X	X		M	M	M	M	4-1		Verify that change-control procedures exist and are used to implement security patches requiring the following:	
X			M	M	M	M	4-2		1. Test all security patches before they are deployed or placed in production.	
X			M	M	M	M	4-3		2. Install new/modified security patches within one month of release, or document reason(s) why it cannot be done.	
			S	R	M	M	4-4		3. Maintain server change control log for a minimum of 6 mos.	
X			M	M	M	M	4-5		Ensure that all operating systems have the appropriate vendor-supplied security patches installed.	
<b>5 - Protect stored data</b>										
	X		R	R	M	M	5-1		Data retention and disposal policies and procedures exist and include the following:	
	X			S	M	M	5-2		1. Legal, regulatory, and business requirements for data retention, (e.g., credit cardholder data needs to be held for X period for Y business reasons).	
	X		S	R	M	M	5-3		2. Dispose of data when no longer needed for legal, regulatory or business reasons.	
	X				R	M	5-4		3. Verify (at least on a quarterly basis) that stored sensitive data does not exceed business retention requirements	

Safeguards <sup>[1]</sup>			Category of Data <sup>[2]</sup>				Item Ref.	Measures <sup>[3]</sup>	Internal Control	Reference
System	Admin	Physical	I	II	III	IV				
X	X					M	5-5		For creditcard information, ensure no CVV2 (security code on reverse-side of card) data is retained.	
X			M	M	M	M	5-6		Encrypt all passwords stored on networked devices.	
X					M	M	5-7	128-bit encryption or SHA1 (or better) required for Cat IV.	Render sensitive stored data unmeaningful by either encryption, hashing, garbling, truncating or other means.	
X				M	M	M	5-8		Documentation of vendor and/or Institute cryptographic solutions where implemented.	
X				M	M	M	5-9		Encryption solutions include emergency recovery of encrypted data where implemented.	
X					R	M	5-10		Physical and logical isolation to protect categorized data.	
X	X		S	R	M	M	5-11		Compliance with applicable standards as well as legal and regulatory controls.	See NIST , FERPA, HIPAA, Graham-Leach Bliely Act
X	X		M	M	M	M	5-12		Protect encryption keys against both disclosure and misuse.	
X	X		M	M	M	M	5-13		Document all electronic encryption key management processes and procedures.	
<b>6 - Encrypt data sent across public networks</b>										
X			R	R	M	M	6-1		Make encryption techniques such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) standard in management of Information Systems domains and file services	
	X				M	M	6-2	(eg. PGP and password-protected attachments)	Never send sensitive data via unencrypted e-mail.	
X					M	M	6-3		Encrypt access to sensitive databases (eg. Passwords, ids, data streams)	
<b>7 - Use and regularly update anti-virus software</b>										
X	X		M	M	M	M	7-1		Use active anti-virus mechanisms with current signatures on all systems.	
X	X		M	M	M	M	7-2		Ensure activity logs are enabled.	
<b>8 - Controlling access based on "need to know "</b>										
X	X	X		S	M	M	8-1		Develop a unit data control procedure that conforms with the Institute Data Access Policy. Limit access to computing resources and sensitive information to only those individuals whose job requires such access.	
	X			S	M	M	8-2		Instruct managers that access rights assigned to privileged User IDs are restricted to least privileges necessary to perform the job.	
X	X			M	M	M	8-3		Only active users with appropriate USERIDs should have access. Inactive accounts should be removed from access lists asap.	
X	X				M	M	8-4		Maintain a written procedure for data access control, and include the following:	
X	X				M	M	8-5		1. All production operating systems, workstations, network components, databases, and applications.	
X	X				M	M	8-6		2. Requirement for an authorization form that is signed by management and specifies required privileges.	

Safeguards <sup>[1]</sup>			Category of Data <sup>[2]</sup>				Item Ref.	Measures <sup>[3]</sup>	Internal Control	Reference
System	Admin	Physical	I	II	III	IV				
<b>9 - Uniquely ID each person or system</b>										
X	X			M	M	M	9-1		Uniquely identify all personnel before creating user accounts allowing them to access system resources.	
			S	M	M	M	9-2		Authenticate all authorized personnel by using the following or comparable methods:	
X			S	M	M	M	9-3		1. Unique user name and password	
X					R	R	9-4		2. Token devices (i.e., Secured, certificates, or public key)	
X	X	X			R	R	9-5		3. Biometrics	
X	X			R	M	M	9-6		Ensure proper user authentication and password management by ensuring the following practices:	
X				M	M	M	9-7		1. Control the addition, deletion, and modification of user IDs, credentials, or other identifier objects.	
X	X			M	M	M	9-8	eg. Scrambling and/or expiring passwords.	2. Immediately disable access for terminated users.	
	X		M	M	M	M	9-9		3. Distribute password procedures and policies to all users.	
X	X					M	9-10		4. Do not permit group or shared user accounts.	
X	X			R	M		9-11		4a. Do not permit group or shared user accounts without approval from Internal Auditing.	
X	X			M	M	M	9-12		5. Change user passwords at least every 90 days.	
X	X			M	M	M	9-13		6. Require a minimum password length of at least 7 characters.	
X	X			M	M	M	9-14		7. Use passwords containing a mix of both numeric, special and alphabetic characters.	
X	X			R	R	M	9-15		8. Do not allow an individual to submit a new password that is the same as any of the last four passwords used.	
X					R	M	9-16		9. Limit "repeated" attempts by locking out the user ID after a specific number of tries. (The maximum number for system access attempts must not exceed six for Cat IV).	
X	X	X	M	M	M	M	9-17		10. Monitor failed system access attempts on a regular basis ( <i>daily for Cat IV data</i> ).	
X						M	9-18		11. Set the lockout duration to "forever" until administrator enables the user ID.	
X				R	M	M	9-19		12. If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal/machine.	
X						M	9-20		Authenticate all access to any database . This includes all applications, administrators, and all other users.	
X				S	M		9-21		Authenticate all access to any database . This includes all applications, administrators, and all other users. Exceptions need to be approved by Internal Auditing.	
<b>10 - System Configuration Practices</b>										
X			M	M	M	M	10-1	For Cat I, II, III, wherever possible.	Always change the vendor-supplied defaults before you install a system or device on the network (i.e., passwords, SNMP community strings, unnecessary accounts, etc.).	

Safeguards <sup>[1]</sup>			Category of Data <sup>[2]</sup>				Item Ref.	Measures <sup>[3]</sup>	Internal Control	Reference
System	Admin	Physical	I	II	III	IV				
X			M	M	M	M	10-2		Develop system configuration standards for all "networks components". Make sure these standards address all known security vulnerabilities and industry best practices.	
X				S	S	M	10-3		1. Implement only one application or primary function per network component (i.e., one application per server).	
X						M	10-4		2. Make sure each network component contains the minimum hardware and software it needs to prevent misuse.	
X	X		M	M	M	M	10-5		3. Disable all unnecessary services.	SANS
X			M	M	M	M	10-6		4. Configure system security parameters to prevent misuse.	
X	X		M	M	M	M	10-7		5. Enable the appropriate audit subsystems	
X			M	M	M	M	10-8	eg. Routers, switches, hubs, bridges, etc.	6. Configure the networking subsystems to protect against known attacks.	
X	X		M	M	M	M	10-9		Establish a process to identify newly discovered security vulnerabilities. Update your standards to address new vulnerability issues.	
<b>11 - Track all access to data by unique ID</b>										
X					R	M	11-1		Establish a process for tracing all data access activities (especially those with root or administrative privileges) to an individual user or system.	
									Implement <b>AUTOMATED</b> audit trails to reconstruct the following events:	
X				S	R	M	11-2		1. All accesses to sensitive data.	
X					M	M	11-3		2. All actions taken by any individual with <b>operating system-level</b> root or administrative privileges	
X					R	M	11-4		2a. All actions taken by any individual with <b>application-level</b> root or administrative privileges	
X					R	M	11-5		3. Access to all audit trails	
X					R	M	11-6	eg. SQL injection monitoring	4. Invalid logical access attempts	
X					M	M	11-7	eg. Successful/failed login attempt monitoring	5. Use of identification and authentication mechanisms	
X				S	M	M	11-8		6. Initialization of the audit logs	
X				S	R	M	11-9		7. Deletion of objects	
X	X				R	M	11-10		8. Actions taken in response to the compromise of cryptographic keys	
X	X				R	M	11-11		Document changes in the custody of keys and devices or media holding keys	
X	X				R	M	11-12		Document all encryption key management operations	
									Record the following audit trail entries for each event:	
X					R	M	11-13		1. User identification	
X					R	M	11-14		2. Type of event	
X					R	M	11-15		3. Date and time	
X					R	M	11-16		4. Success or failure indication	

Safeguards <sup>[1]</sup>			Category of Data <sup>[2]</sup>				Item Ref.	Measures <sup>[3]</sup>	Internal Control	Reference
System	Admin	Physical	I	II	III	IV				
X					R	M	11-17	eg. IP address	5. Origination of event	
X					R	M	11-18		6. Identity or name of affected data, system component, or resource	
X					R	M	11-19		Secure audit trails so they cannot be altered in any way, e.g. writing to CD-R or storing logs on a physically and logically separated server.	
X			R	R	M	M	11-20		Review security, firewall, and server logs on a regular basis ( <i>daily for Cat IV data</i> ).	
<b>12 - Regularly test security systems and processes</b>										
X	X		M	M	M	M	12-1	Also see line 47	Run internal vulnerability scans at least monthly and external network vulnerability scans at least semi-annually and after any change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades).	
X	X		R	R	M	M	12-2		Before promoting custom application code to the production site, review it carefully to identify any potential coding vulnerability.	
X	X				R	M	12-3		Perform penetration testing on network infrastructure and applications at least once a year and after any "significant" infrastructure and application upgrade or modification (e.g., operating system upgrade, sub-network added to environment, web server added to environment, etc.).	
X	X		M	M	M	M	12-4		Use network intrusion detection systems to monitor all network traffic and alert personnel to suspected compromises.	
X	X		R	R	M	M	12-5		Designate specific personnel to be available for contact on a 24/7 basis in case of unexpected compromises.	
X	X					M	12-6		Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files.	
X	X					M	12-7		Designate specific personnel to be available on a 24/7 basis to respond to reports of unauthorized sensitive system or content file changes.	
X	X		M	M	M	M	12-8		Be prepared to respond immediately to a <b>system failure</b> , as directed in the business system recovery plan.	
X	X		M	M	M	M	12-9		1. Maintain a business and disaster recovery plan that involves a crisis-management team who can handle all mission-critical decisions, if possible together during a moment of crisis.	
X	X		M	M	M	M	12-10		2. Test the plan at least annually.	
	X		M	M	M	M	12-11		3. Appropriately train faculty and staff on operational business and recovery plan execution responsibilities.	
X	X		R	R	M	M	12-12		Be prepared to respond immediately to a <b>system breach</b> .	
X	X		M	M	M	M	12-13		1. Create a plan that designates roles and responsibilities in the event of system compromise. Make sure the plan addresses security communication/contract strategies (e.g., informing Visa, law enforcement, internal parties, etc.).	
X	X		M	M	M	M	12-14		2. Test the plan at least annually.	
	X		M	M	M	M	12-15		3. Adequately train faculty and staff with security breach response responsibilities.	

**Data Protection Safeguards**

Safeguards <sup>[1]</sup>			Category of Data <sup>[2]</sup>				Item Ref.	Measures <sup>[3]</sup>	Internal Control	Reference
System	Admin	Physical	I	II	III	IV				
X	X		S	R	R	M	12-16		Make sure media is backed up nightly to adequately facilitate recovery. Store media back-ups in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.	