Information Security Program & Compliance Reference

Release	2017-02-23
Document status	LIVE
Document owner	Chief Information Officer

GLBA/NIST

Guidelines: Dept Ed Dear Colleague Letter, 2019-Oct-30

Required procedures per 2019-Oct-30 Dear Colleague letter:

- C.8.12.a. Verify that the institution has designated an individual to coordinate the information security program.
  (See Title IV Information Security Program Responsibilities)
- C.8.12.b. Verify that the institution has performed a risk assessment that addresses the three required areas noted in 16 CFR 314.4(b), which are
  - (1) Employee training and management;
  - (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
  - (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
    (See Security Safeguards Program: Title IV Data)
- C.8.12.c. Verify that the institution has documented a safeguard for each risk identified from step b above.
  (See Security Safeguards Program: Title IV Data)

DLP: LETU Data Loss Protection System

FERPA/HIPAA

FERPA/HIPAA Resources

- Guidelines: https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf

Additional Resources

- Security Awareness Program: Title IV Data
- Security Safeguards Program: Title IV Data
- Title IV: Department of Education Requirements
- Title IV: How Do I Report a Breach
- Title IV Information Security Program Responsibilities

Controls

ISO	Payment Card Industry	Gramm-Leach-Bliley Act	NIST	Financial Audit	LETU
27002: 2005	PCI DSS 3.2	GLBA	SP 800-171 r1		Compliance Controls

Section 4: Risk Assessment & Treatment

4.1 **Assessing Security Risks** Identify, quantify, and prioritize risks against criteria for risk acceptance relevant to the organization • Performed Periodically • Systematic Approach estimating risks • Clearly defined scope	PCI is an audit standard and risks are quantified and prioritized within it *Maintain an Information Security Policy* 12.2 - Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk	III.B. Assess Risk	N/A		**Trustwave PCI Rapid Comply** PCI compliance scanner: pcirapidcomply2.com used monthly. **Server Vulnerability Scans** Servers scanned on a regular basis using Tenable.io vulnerability scanning tool. **DLP Compliance** DLP Compliance polices (currently active on all LETU O365-enabled accounts) alert on shared content for users which could compromise compliance with PCI, GLBA or other Privacy or Financial regulations. This includes email for users converted to LETU's O365 email platform. **Network Compliance** LETU Network Mgmt System is configured to trigger alerts and guidance on detected issues or vulnerabilities affecting compliance with best practices or regulatory issues within LETU's network architecture. These alerts trigger configuration team reviews and modifications as needed. **Title IV: Department of Education Requirements** **NIST Framework for Improving Critical Infrastructure Cybersecurity** LETU evaluates internal CyberSecurity measures against NIST Framework v1.1 as part of internal annual CyberSecurity review process
4.2 **Treating Security Risks** Before treating, organization must ascertain ability and level of risk acceptable to an organization • Knowing and objectively accepting risk in accordance with organization risk tolerance • Avoiding risk by not engaging in activities that introduce risk • Transferring risks to other parties	*Protect Cardholder Data* 3.4 - Render PAN (Primary Account Number), at a minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) 6 - Develop and maintain secure systems and applications	III.C. Manage and Control Risk	N/A		All data at rest stored using one-way strong encryption hashes **Cardholder Data** PAN information is not stored on LETU systems. All external vendors required to comply with PCI DSS standards. LETU Maintains PCI Compliant status. **MFA** Mandatory multi-factor authentication for all LETU employees eliminates threat of single-factor password compromises.
Section 5: Security Policy					
5.1 **Information Security Policy** Information security policies should be sponsored/approved by management, published to all employees and relevant external parties Include within: • Definition of information security, objectives, scope, and importance • Statement of management intent, supporting goals and principles • Framework for setting control objectives and controls	*Maintain an Information Security Policy* 12.4 - Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors 12.5.1 - Establish, document, and distribute security policies and procedures	II.A. Information Security Program II.B. Objectives III.A. Invoice Board of Directors	N/A	**Security** f. Information Security policy	**LETU Information Security Compliance Reference** LETU Information Security Compliance Reference reviewed by Information Security office annually and employees reminded annually. **Title IV: Department of Education Requirements**
Section 6: Organization of Information Security					
6.1 **Internal Organization** A management framework should be established to initiate and control the implementation of information security within the organization	*Maintain an Information Security Policy* 12.4 - Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors. 12.5.1 - Establish, document, and distribute security policies and procedures	II. A. Information Security Program II.B. Objectives III. A. Involve the Board of Directors III.C. Manage and Control Risk III.F. Report to the Board	3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion 3.6 Incident Response 3.14 System and Information Integrity		**LETU Information Security Compliance Reference** LETU Information Security Compliance Reference reviewed by Information Security office annually and employees reminded annually. **Security Awareness Program: Cardholder Data** **Title IV: Department of Education Requirements**

6.2 **External Parties** To maintain the security of information and information processing facilities that are accessed, processed, communicated to, or managed by external parties	*Maintain an Information Security Policy* 12.8.2 - Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers posess	III.C. Manage and Control Risk III.D. Oversee Service Provider Arrangements	3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) 3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute		**Statements of Service Provider Compliance: PCI**
Section 7: Asset Management					
7.1 **Responsibility for Assets** All assets should be accounted for and have a nominated owner	*Maintain an Information Security Policy* 12.3.4 Labeling of devices with owner, contact information, and purpose	N/A	3.1.21 Limit use of organizational portable storage devices on external information systems 3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems throughout their life cycle 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems 3.9 Personnel Security		**Card Devices** Physical labeling and annual inspection of card devices for payment card industry cards. **Network Equip** All LETU network equipment physically tagged and inventoried for tracking purposes. **System Center Configuration Manager** Used to tattoo funding agent responsible for asset and to inventory asset information to central database
7.2 **Information Classification** Information should be classified to indicate the need, priorities and expected degree of protection • Define an information classification scheme	*Implement Strong Access Control Measures* 7.1 - Limit access to system components and cardholder data to only those individuals whose job requires such access. 7.2 - Establish an access control system for system components with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	PII (Personal Indentifying Information) is protected here.	3.8 Media Protection 3.13.1 Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems		**Datacenter Security Measures** All LETU Datacenters containing protected information are secured by proximity-based card access control systems with highly restrictive access configurations as well as video security coverage with archival review capabilities. Access to all LETU Datacenters is extremely limited. More information is available in the LETU Datacenter Security Guidelines document. **Network ACLs** Network Access Control lists (ACLs) are used to restrict access to systems based on IP, port or other network characteristic and is used to restrict access to locations from which access is expected to originate. **Security Groups** Security Groups are used to restrict access to specific content on a per-user basis as authorized by the primary owner of the data or content. **Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf
Section 8: Human Resources Security					
8.1 **Prior to Employment** To ensure that employees, contractors and third party users understand responsibilities, and are suitable for their roles; reduce the risk of theft, fraud, and or misuse of facilities/ resources	*Maintain an Information Security Policy* 12.7 - Screen potential employees prior to hire to minimize the risk of attacks from internal sources.	III.C. Manage and Control Risk	3.9.1 Screen individuals prior to authorizing access to information systems containing CUI		**Human Resources** Background checks are performed on all new-hires

8.2 **During Employment** To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support security policy in the course of their normal work	*Maintain an Information Security Policy* 12.6 - Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	III.C. Manage and Control Risk	3.2 Awareness and Training 3.6 Incident Response	**Systems Development and Change Management** c. Policies regarding system development, program change **Security** i. Procedures for issuing and suspending user access	**New-Hire training** IT orientation with all new employees to brief them on cybersecurity best practices **DLP Compliance** DLP Compliance polices (currently active on all LETU O365-enabled accounts) alert on shared content for users which could compromise compliance with PCI, GLBA or other Privacy or Financial regulations. This includes email for users converted to LETU's O365 email platform. **Self-Phishing Campaigns** Quarterly self-phishing conducted with email training sent to all employees **Annual PCI training** Yearly PCI training emailed to employees directly involved in credit card processing **Program Change** IT Directors review training needs during annual performance reviews. Employees offered training as new software is made available **Annual Re-Authorization** Each year access rights are periodically reviewed by every supervisor and must be reauthorized to maintain those rights for the upcoming year
8.3 **Termination or Change of Employment** To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner	*Implement Strong Access Control Measures* 9.3 - Immediately revoke access for any terminated users *Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	N/A	3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers	**Security** i. Procedures for suspending and closing user accounts	**Account Automation** In-house programmatic account access control used to disable accounts keyed off an employee's separation date in an HR database **Separation Process** Human Resource notifications to IT trigger a specific review of each separation, tracked using our WIT request system for additional specific review of the security and other IT needs related to each separation.
Section 9: Physical and Environmental Security					
9.1 **Secure Areas** To prevent unauthorized physical access, damage, and interference to the organization's premises and information • Critical or sensitive information processing facilities should be housed in secure areas • Protection provided should be commensurate with the identified risks	*Implement Strong Access Control Measures* 9. Restrict physical access to cardholder data	III.C. Manage and Control Risk	3.10 Physical Protection	**Security** j. Physically restrict access to key components	**Datacenter Security Measures** All LETU Datacenters containing protected information are secured by proximity-based card access control systems with highly restrictive access configurations as well as video security coverage with archival review capabilities. Access to all LETU Datacenters is extremely limited. The Data Center has its own environmental control (AC) as well as Uninterruptible Power Supply (UPS). Fire extinguishers are present in both data centers. Email alerts go out with detection of excessive heat More information is available in the LETU Datacenter Security Guidelines document.
9.2 **Equipment Security** To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities	*Implement Strong Access Control Measures* 9.1.3 - Restrict physical access to wireless access points, gateways, and handheld devices	III.C. Manage and Control Risk	3.7 Maintenance 3.8 Media Protection 3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites)		**Locked AP cabinets** Wireless Access Points located in locked enclosures **Unauthorized WAP detection** Detection and Identification of Unauthorized Wireless Access Points (WAPs) **Datacloset Security Measures** All LETU Dataclosets are secured with a non-general-master keyset and most are additionally secured by proximity-based electronic locking systems. **Datacenter Security Measures** All LETU Datacenters containing protected information are secured by proximity-based card access control systems with highly restrictive access configurations as well as video security coverage with archival review capabilities. Access to all LETU Datacenters is extremely limited. More information is available in the LETU Datacenter Security Guidelines document.
Section 10: Communications and Operations Management					
10.1 **Operational Procedures & Responsibilities** Responsibilities and procedures for the management and operation of all information processing facilities should be established • Segregation of duties should be implemented	6.4.1 - Separate development /test and production environments	III.C. Manage and Control Risk	3.4.3 Track, review, approve /disapprove, and audit changes to information systems 3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system		**LETU Production/Test Architecture** LETU maintains specific testing environments separate from the production environment as necessary for the secure evaluation of development or updated code /configs on both LETU virtual server hosting systems and network architecture. Access lists and secured credentials limit access to both production and testing environment resources to authorized users. **Title IV: Department of Education Requirements**

10.2 **Third-Party Service Delivery Management** Validate the implementation of agreements, monitor compliance, and manage changes to ensure that all services delivered meet requirements set out in agreements	*Maintain an Information Security Policy* 12.8.2 Maintain a written agreement that includes acknowledgement that the service providers are responsible for the security of cardholder data the service providers posses.	III.D. Oversee Service Provider Arrangements	N/A		**Statements of Service Provider Compliance: PCI**
10.3 **System Planning and Acceptance** To minimize the risk of systems failures • Advanced planning and preparation are required to ensure availability and adequate capacity of resources • Operational requirements of new systems should be established, documented, and tested	*Maintain a Vulnerability Management Program* 6. Develop and maintain secure systems and applications *Regularly Monitor and Test Networks* 11. Regularly test security systems and processes	III.C. Manage and Control Risk	N/A		**Trustwave PCI Rapid Comply** PCI compliance scanner: pcirapidcomply2.com used monthly. **Server Vulnerability Scans** Public-facing servers scanned annually using https://www.ssllabs.com/ssltest tool. **DLP Compliance** DLP Compliance polices (currently active on all LETU O365-enabled accounts) alert on shared content for users which could compromise compliance with PCI, GLBA or other Privacy or Financial regulations. This includes email for users converted to LETU's O365 email platform. **Network Compliance** LETU Network Mgmt System is configured to trigger alerts and guidance on detected issues or vulnerabilities affecting compliance with best practices or regulatory issues within LETU's network architecture. These alerts trigger configuration team reviews and modifications as needed. **Data Loss Preventation Guidelines**
10.4 **Protection Against Malicious & Mobile Code** Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code	*Maintain a Vulnerability Management Program* 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications	III.C. Manage and Control Risk	3.2 Awareness and Training 3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems 3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response 3.14.4 Update malicious code protection mechanisms when new releases are available 3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed		**System Center Endpoint Protection** Protects against malicious code for managed endpoints; new definitions are automatically downloaded daily and real-time protection is enabled on all managed clients along with daily quick-scans and weekly full-scans
10.5 **Back-up** To maintain the integrity and availability of information and information processing facilities	*Implement Strong Access Control Measures* 9. Restrict physical access to cardholder data *Regularly Monitor and Test Networks* 10. Track and monitor all access to network resources and cardholder data *Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk	3.8.9 Protect the confidentiality of backup CUI at storage locations	**Operations** h. Recorded data remains complete and accurate	**Veeam** Disaster recovery for all managed virtual servers **Backup Exec** Disaster recovery for additional agent-managed servers **\\letnet.net\fs\backup Backups** Disaster recovery for non-agent, *nix-based and other systems **Off-site** Regularly rotated Off-site vault storage of backup media

10.6 **Network Security Management** To ensure the protection of information in networks and the protection of the supporting infrastructure	*Build and Maintain a Secure Network* 1. Install and maintain a firewall 2. Do not use vendor-supplied defaults for system passwords and other security parameters *Maintain a Vulnerability Management Program* 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications	III.C. Manage and Control Risk	3.1.2 Monitor and control remote access sessions 3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions 3.1.14 Route remote access via managed access control points 3.1.16 Authorize wireless access prior to allowing such connections 3.1.17 Protect wireless access using authentication and encryption 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete 3.13 System and Communications Protection	**Security** h. Network security restricts access to financial systems	**Gateway Security** LETU networks are secured with access control lists (ACLs) ACLs that greatly restrict access **to all LETU** **MFA** Mandatory multi-factor authentication for all LETU employees eliminates threat of single-factor password compromises. **System Center Configuration Manager** Inventory and manage technology assets throughout lifecycle to ensure security **System Center Endpoint Protection** Protects against malicious code for managed endpoints
10.7 **Media Handling** To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities • Media should be controlled and physically protected • Appropriate operating procedures should be established to protect, documents, and computer media	*Protect Cardholder Data* 3. Protect stored data 4. Encrypt transmissions of cardholder data and sensitive information across public networks *Implement Strong Access Control Measures* 7. Restrict access to data by business need-to-know 9. Restrict physical access to cardholder data *Regularly Monitor and Test Networks* 11. Regularly test security systems and processes *Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk	N/A		Protect Stored Cardholder Data Encrypt transmission of cardholder data across open, public networks **Mobile Device Encryption** All mobile devices have encrypted hard drives per LETU policy: http://www.letu.edu/start/publications/policy/upps/mobile-encryption.pdf
10.8 **Exchange of Information** To maintain the security of information and software exchanged within an organization and with any external entity	*Build and Maintain a Secure Network* 1. Install and maintain a firewall Protect Cardholder Data: 4. Encrypt transmissions of cardholder data and sensitive information across public networks *Implement Strong Access Control Measures* 7. Restrict access to data by business need-to-know *Implement Strong Access Control Measures* 8. Assign a unique ID to each person with computer access *Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk	3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information 3.1.16 Authorize wireless access prior to allowing such connections 3.1.17 Protect wireless access using authentication and encryption 3.13 System and Communications Protection		**Unique IDs** Each user has a unique SIS ID and username **Role-Based Access** Each employee given access and appropriate permissions only to systems to which they need those specific rights Customer request system allows supervisors to request permissions their employees need. **Data Loss Prevention (DLP)**

10.9 **Electronic Commerce Services** To ensure the security of electronic commerce services, and their secure use	*Build and Maintain a Secure Network* 1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters *Protect Cardholder Data* 4. Encrypt transmissions of cardholder data and sensitive information across public networks *Maintain a Vulnerability Management Program* 6. Develop and maintain secure systems and applications	III.C. Manage and Control Risk	N/A	**Operations** l. Ensure third-party services are secure	**Trustwave PCI Rapid Comply** PCI compliance scanner: pcirapidcomply2.com used monthly. **Qualys SSL Labs** Server security scanner: https://www.ssllabs.com/ssltest used annually Encrypt transmission of cardholder data across open, public networks **Vendor Guidelines** Established guidelines in place when selecting on-premise or cloud-hosted vendor applications. Contracts for these vendors are reviewed by CIO and CFO with questions specific to risks, security controls, and other guideline-based information. This policy is contained in the Acceptable Use for Technology Systems. **Acceptable Use for Technology Systems** http://www.letu.edu/start/publications/policy/letu-policy-handbook.pdf **Data Loss Prevention (DLP)**
10.10 **Monitoring** To detect unauthorized information processing activities including review of operator logs and fault logging • Systems should be monitored and information security events should be recorded • Organization should comply with all relevant legal requirements applicable to monitoring and logging • System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to access policies	*Implement Strong Access Control Measures* 8.1.1 Assign a unique ID to each person with computer access *Regularly Monitor and Test Networks* 10. Track and monitor all access to network resources and cardholder data	III.C. Manage and Control Risk	3.3 Audit and Accountability	**Operations** n. Procedures for job scheduling, processing, error monitoring, system availability	**Unique IDs** Each user has a unique SIS ID and username **Role-Based Access** Each employee given access and appropriate permissions only to systems to which they need those specific rights Customer request system allows supervisors to request permissions their employees need. **Technical Monitoring** Many systems in place including central log aggregation, monitoring solutions, and custom scripts. Email/text alerts generated upon threshold for any monitor
Section 11: Access Control					
11.1 **Business Requirement for Access Control** Access to information, information processing facilities, and business processes should be controlled based upon business and security requirements. • Access controls should take account policies for information dissemination and authorization	*Implement Strong Access Control Measures* 8.1.1 Assign a unique ID to each person with computer access *Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk	3.1 Access Control		**Unique IDs** Each user has a unique SIS ID and username **Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf
11.2 **User Access Management** Formal procedures to control the allocation of access rights to information systems and services	*Implement Strong Access Control Measures* 7. Restrict access to data by business need-to-know 8.1.1 Assign a unique ID to each person with computer access	III.C. Manage and Control Risk	3.1 Access Control 3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system 3.5 Identification and Authentication	**Entity-Level Controls** b. Segregation of responsibilities to prevent subversion of critical processes	**Unique IDs** Each user has a unique SIS ID and username **Role-Based Access** Each employee given access and appropriate permissions only to systems to which they need those specific rights Customer request system allows supervisors to request permissions their employees need. **Segregation of Responsibilities** Personnel are prohibited from engaging in user activities, initiating transactions, or changing master files. IT personnel prevented from having access to liquid assets such as check signing approval or credit approval. eBridge Access
11.3 **User Responsibilities** To prevent unauthorized user access, and compromise or theft of information and information processing capabilities	*Build and Maintain a Secure Network* 2. Do not use vendor-supplied defaults for system passwords *Implement Strong Access Control Measures* 8.1.1 Assign a unique ID to each person with computer access *Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk	N/A		**Non-Default Credentials** Passwords for built-in accounts never left at default **Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf **LetNet Guest Wireless Account Creation** Guest account policies direct use of specific individual account information for each guest.

11.4 **Network Access Control** Ensure that appropriate interfaces and authentication mechanisms to networked services are in place	*Build and Maintain a Secure Network* 2. Do not use vendor-supplied defaults for system passwords *Implement Strong Access Control Measures* 8.1.1 Assign a unique ID to each person with computer access	III.C. Manage and Control Risk	3.1.9 Provide privacy and security notices consistent with applicable CUI rules 3.1.16 Authorize wireless access prior to allowing such connections 3.1.20 Verify and control/limit connections to and use of external information systems		**Non-Default Credentials** Passwords for built-in accounts never left at default **Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf **LetNet Guest Wireless Account Creation** Guest account policies direct use of specific individual account information for each guest.
11.5 **Operating System Access Control** To prevent unauthorized access to operating systems Some methods include: ensure quality passwords, user authentication, and the recording of successful and failed system accesses, providing appropriate authentication control means	*Build and Maintain a Secure Network* 2. Do not use vendor-supplied defaults for system passwords *Implement Strong Access Control Measures* 8.1.1 Assign a unique ID to each person with computer access *Monitor and Test Networks* 10. Track and monitor all access to network resources and cardholder data	III.C. Manage and Control Risk	3.1.8 Limit unsuccessful logon attempts 3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system	**Security** g. Financial operating systems appropriately secured	**Non-Default Credentials** Passwords for built-in accounts never left at default **Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf **LETNET Domain Password Requirements** Last 24 unique password history enforced Annual password change (Faculty/Staff) 7 character minimum Complexity requirement: 3/4 character groups (Upper, Lower, Number, Symbol) Non-reversible password hash encryption Account lockout after 5 invalid logon attempts within 15 mins Audits for all failed logon events
11.6 **Application and Information Access Control** • To prevent unauthorized access to information held in application systems • Security facilities should be used to restrict access to an within application systems • Logical access to application software and information system functions	*Build and Maintain a Secure Network* 1. Do not use vendor-supplied defaults for system passwords *Maintain a Vulnerability Management System* 6. Develop and maintain secure systems and applications *Implement Strong Access Control Measures* 8.1.1 Assign a unique ID to each person with computer access	III.C. Manage and Control Risk	3.1.21 Limit use of organizational portable storage devices on external information systems 3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system 3.5 Identification and Authentication		**Unique IDs** Each user has a unique SIS ID and username **Role-Based Access** Each employee given access and appropriate permissions only to systems to which they need those specific rights
11.7 **Mobile Computing and Teleworking** To ensure information security when using mobile computing and teleworking facilities	*Build and Maintain a Secure Network* 1. Install and maintain a firewall configuration to protect data *Build and Maintain a Secure Network* 2. Do not use vendor-supplied defaults for system passwords and other security parameters *Implement Strong Access Control Measures* 8. Assign a unique ID to each person with computer access	III.C. Manage and Control Risk	3.1.12 Monitor and control remote access sessions 3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions 3.1.14 Route remote access via managed access control points 3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information 3.1.18 Control connection of mobile devices 3.1.19 Encrypt CUI on mobile devices 3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites)		**Unique IDs** Each user has a unique SIS ID and username **Role-Based Access** Each employee given access and appropriate permissions only to systems to which they need those specific rights **Firewall** OS-level firewalls enabled on each client along with hardware firewalls at edge of LETU network **Mobile Device Encryption** All mobile PCs required to have full-disk encryption: http://www.letu.edu/start/publications/policy/upps/mobile-encryption.pdf
Section 12: Information Systems Acquisition, Development and Maintenance					

12.1 **Ensure that security is an integral part of information systems** Security should be built into operating systems, infrastructure, business applications, off the shelf products, and user-developed applications	*Maintain a Vulnerability Management Program* 6. Develop and maintain secure systems and applications	N/A	3.1.20 Verify and control/limit connections to and use of external information systems 3.13 System and Communications Protection		**Trustwave PCI Rapid Comply** PCI compliance scanner: pcirapidcomply2.com used monthly. **Server Vulnerability Scans** Public-facing servers scanned annually using https://www.ssllabs.com/ssltest tool. **DLP Compliance** DLP Compliance polices (currently active on all LETU O365-enabled accounts) alert on shared content for users which could compromise compliance with PCI, GLBA or other Privacy or Financial regulations. This includes email for users converted to LETU's O365 email platform. **Network Compliance** LETU Network Mgmt System is configured to trigger alerts and guidance on detected issues or vulnerabilities affecting compliance with best practices or regulatory issues within LETU's network architecture. These alerts trigger configuration team reviews and modifications as needed.
12.2 **Correct Processing in Applications** To prevent errors, loss, unauthorized modification or misuse of information in applications	*Maintain a Vulnerability Management Program* 6. Develop and maintain secure systems and applications	III.C. Manage and Control Risk	N/A		**Trustwave PCI Rapid Comply** PCI compliance scanner: pcirapidcomply2.com used monthly. **Server Vulnerability Scans** Public-facing servers scanned annually using https://www.ssllabs.com/ssltest tool. **DLP Compliance** DLP Compliance polices (currently active on all LETU O365-enabled accounts) alert on shared content for users which could compromise compliance with PCI, GLBA or other Privacy or Financial regulations. This includes email for users converted to LETU's O365 email platform. **Network Compliance** LETU Network Mgmt System is configured to trigger alerts and guidance on detected issues or vulnerabilities affecting compliance with best practices or regulatory issues within LETU's network architecture. These alerts trigger configuration team reviews and modifications as needed.
12.3 **Cryptographic Controls** • To protect the confidentiality, authenticity or integrity of information by cryptographic means • Policy should be developed on the use of cryptographic controls • Key management should be in place to support cryptographic techniques	*Protect Cardholder Data* 3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks	III.C. Manage and Control Risk	3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions 3.1.17 Protect wireless access using authentication and encryption 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission 3.13.10 Establish and manage cryptographic keys for cryptography employed in the information system 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI		Remote Services for Remote offices and Employees protected by mandatory Encryption [ref] All data at rest on mobile or physically insecure devices stored using one-way strong encryption hashes **Kerberos Policy** Kerberos tickets are enforced for domain clients through Group Policy which ensures: 600 minute service ticket lifetime; 10 hour user ticket lifetime; 5 minute tolerance for computer clock synchronization **Certificate Authority** On-campus domain certification authority handles automatic certificate management on domain-joined clients
12.4 **Security of System Files** To ensure security of system files through the control of access to system files and program source code	*Build and Maintain a Secure Network* 2. Do not use vendor-supplied defaults for system passwords and other security parameters	III.C. Manage and Control Risk	N/A		**Non-Default Credentials** Passwords for built-in accounts never left at default

12.5 **Security in Development and Support Processes** Project and support environments should be strictly controlled	*Maintain a Vulnerability Management Program* 6. Develop and maintain secure systems and applications	N/A	3.1.14 Route remote access via managed access control points 3.4.3 Track, review, approve /disapprove, and audit changes to information systems 3.4.4 Analyze the security impact of changes prior to implementation 3.12 Security Assessment	**Systems Development and Change Management** d. Acquiring, implementing, integrating, and maintaining IS applications e. Acquiring, implementing, integrating, and maintaining infrastructure	**Role-Based Access** Each employee given access and appropriate permissions only to systems to which they need those specific rights **Change Management** IT Business Systems team receives notifications of patches and hotfixes, and reviews related release notes. This team then requests approval from change management team for a time to perform updates. Full databases and system backups are done nightly. Tape rotation method is used to allow complete recovery. Complete backups are performed prior to any new or updated application being deployed.
12.6 **Technical Vulnerability Management** To reduce risks resulting from exploitation of published technical vulnerabilities • Technical vulnerability management should be effective, systematic, and repeatable	*Maintain a Vulnerability Management Program* 5. Use and regularly update antivirus software 6. Develop and maintain secure systems and applications	III.C. Manage and Control Risk	3.11 Risk Assessment		**System Center Endpoint Protection** Protects against malicious code for managed endpoints and new definitions are automatically downloaded daily **RSS/Web Lists** RSS, mailing lists, and forums are used to keep apprised of newly published vulnerabilities. Manual patches are tracked through collaborative spreadsheets until stakeholders have verified each affected endpoint has been patched **Trustwave PCI Rapid Comply** PCI compliance scanner: pcirapidcomply2.com used annually **Qualys SSL Labs** Server security scanner: https://www.ssllabs.com/ssltest used annually
Section 13: Information Security Incident Management					
13.1 **Information Security Incident Management** To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken • Formal event reporting and escalation procedures should be in place	*Maintain a Vulnerability Management Program* 6. Develop and maintain secure systems and applications *Regularly Monitor and Test Networks* 11. Regularly test security systems and processes Maintain an Information Security Policy: 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk	3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) 3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute 3.1.3 Control the flow of CUI in accordance with approved authorizations	**Operations** m. Process for identifying and resolving incidents	**Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf **Communication Policy** Defines response expectations for various incidents: Communication Policy **Incident Log** Incident Log **Department of Ed Notification** Special notification requirement for Title IV data breach.

13.2 **Management of Information Security Incidents and Improvements** • To ensure a consistent and effective approach is applied to the management of information security incidents	*Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk	3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) 3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute 3.1.3 Control the flow of CUI in accordance with approved authorizations 3.3 Audit and Accountability 3.6 Incident Response	**Security** f. Information Security policy	**Communication Policy** Defines response expectations for various incidents: Communication Policy **Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf
Section 14: Business Continuity Management					
14.1 **Information Security Aspects of Business Continuity Management** To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters and to ensure their timely resumption	*Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk	3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) 3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute 3.1.3 Control the flow of CUI in accordance with approved authorizations 3.8.9 Protect the confidentiality of backup CUI at storage locations	**Entity-Level Controls** a. Plans that align business objectives with IT strategies	**Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf **Business Objective Alignment** IT-related risks communicated through IT personnel and brought to the attention of CIO. Action plans with due dates are implemented for recovery. Users required to sign confidentiality agreements before any access to administrative software is granted.
Section 15: Compliance					
15.1 **Compliance with Legal Requirements** To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements	*Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk III.F. Report to the Board	3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion 3.3.9 Limit management of audit functionality to a subset of privileged users 3.8.9 Protect the confidentiality of backup CUI at storage locations		**Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf This wiki page reviewed by Information Security office and emailed out as a reminder to all employees annually **Department of Ed Notification** **Title IV: Department of Education Requirements**
15.2 **Compliance with Security Policies and Standards, and Technical Compliance** To ensure compliance of systems with organizational security policies and standards	*Regularly Monitor and Test Networks* 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes *Maintain an Information Security Policy* 12. Maintain a policy that addresses information security for employees and contractors	III.C. Manage and Control Risk III.E. Adjust the Program III.F. Report to the Board	N/A		**Data Classification Standard** http://www.letu.edu/start/publications/policy/upps/dataclassification.pdf **Trustwave PCI Rapid Comply** PCI compliance scanner: pcirapidcomply2.com used monthly. **Qualys SSL Labs** Server security scanner: https://www.ssllabs.com/ssltest used annually Protect Stored Cardholder Data Encrypt transmission of cardholder data across open, public networks

Questions

Below is a list of questions to be addressed as a result of this requirements document:

Question	Outcome
How can we make IT more aware of this information?	Communicate the URL via departmental email

Definitions

CUI - Controlled Unclassified Information. A subset of Federal data that includes unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Federal policies.

Goals

- Provide a single reference for all Information controls in adherence at LETU
- Demonstrate evidence of requirements compliance from organizations such as PCI and DOE

References

PCI: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1483737774239
Layout: https://library.educause.edu/~/media/files/library/2010/3/csd5876-pdf.pdf
NIST SP 800-171: https://library.educause.edu/~/media/files/library/2016/4/nist800.pdf
PCI-DSS to ISO 27002 mapping: Mapping_Document.pdf