Access Control Policy

Policy Title:
Access Control Policy

Responsible Executive(s):
Jim Pardonek, Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This policy applies to Loyola University Chicago faculty, staff, students, contractors, and vendors that connect to servers, applications or network devices that contain or transmit Loyola Protected Data, per the Data Classification Policy. In addition, please note that this policy covers all IoT devices. All servers, applications or network devices that contain, transmit or process Loyola Protected Data are considered "High Security Systems".

Access controls are designed to minimize potential exposure to the University resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of the University networks, systems, and applications.

II. Definitions

VPN: A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

PCI: A set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. It was launched on September 7, 2006, to manage PCI security standards and improve account security throughout the transaction process. An independent body created by Visa, MasterCard, American Express, Discover, and JCB, the PCI Security Standards Council (PCI SSC) administers and manages the PCI DSS.

FERPA: A federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student").

HIPAA: A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

III. Policy

Segregation of Duties

Access to High Security Systems will only be provided to users based on business requirements, job function, responsibilities, or need-to-know. All additions, changes, and deletions to individual system access must be approved by the appropriate supervisor and the UISO, with a valid business justification. Access controls to High Security Systems are implemented via an automated control system. Account creation, deletion, and modification and access to protected data and network resources is completed by the Server Operations group.
Annually, the University Information Security Office will audit all user and administrative access to High Security Systems. Discrepancies in access will be reported to the appropriate supervisor in the unit responsible and remediated accordingly.

User Account Access

User Access:
All users of High Security Systems will abide by the following set of rules:

- Users with access to High Security Systems will utilize a separate unique account, different from their normal University account. This account will conform to the following standards:
  - The password will conform, at a minimum, to the published ITS Password Standards.
  - Inactive accounts will be disabled after 90 days of inactivity.
  - Access will be enabled only during the time period needed and disabled when not in use.
  - Access will be monitored when the account is in use.
  - Repeated access attempts will be limited by locking out the user ID after not more than six attempts.
  - Lockout duration must be set to a minimum of 30 minutes or until an administrator enables the user ID.
  - If a session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.
- Users will not login using generic, shared or service accounts.
- Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

RemoteApp Access
Users may only gain access to the RemoteApp environment if:

- A user's manager must submit the request.

- The Director, Cash Management, Assistant Director, Cash Management or Sr. Treasury Analyst, eCommerce must approve all requests.
- Users will abide by the above user access guidelines.
- Users must complete annual PCI training through the Treasurer's Office.
- Password reset requests must be submitted to the Treasurer's Office and verified with the user's manager.

Administrative Access

- Administrators will abide by the Privileged Access Policy.
- Users will abide by the above user access guidelines.
- Administrators will immediately revoke all of a user's access to High Security Systems when a change in employment status, job function, or responsibilities dictate the user no longer requires such access.
- All service accounts must be used by no more than one service, application, or system.
- Administrators must not extend a user group's permissions in such a way that it provides inappropriate access to any user in that group.
- All servers, applications and network devices shall contain a login banner that displays the following content:
    - "This computer and network are provided for use by authorized members of the Loyola community. The use of this computer and network are subject to all applicable Loyola policies, including Information Technology Services policies, and any applicable Loyola Handbooks. Any use of this computer or network constitutes acknowledgment that the user is subject to all applicable policies. Any other use is prohibited. Users of any networked system, including this computer, should be aware that due to the nature of electronic communications, any information conveyed via a computer, or a network may not be private. Sensitive communications should be encrypted or communicated via an alternative method."

Remote Access

All users and administrators accessing High Security Systems must abide by the following rules:

- No modems or wireless access points are allowed on high security networks, or other unapproved remote access technology.
- All remote access must be authenticated and encrypted through the University's VPN, Loyola Secure Access (LSA).
- All remote access will be accomplished through the use of two factor authentication; a username and password or PIN combination, and a second method not based on user credentials, such as a certificate or token, provisioned to the user.
- Any machine used for remote access must have antivirus and host-based firewall software installed, running, and enabled. This requirement is enforced by a host

checker component of the University's VPN software, and remote access to the High Security Network is only possible after a machine has passed these configured checks.

- Any third-party, non-Loyola affiliate that requires remote access to High Security Systems for support, maintenance or administrative reasons must designate a person to be the Point of Contact (POC) for their organization. In the event the POC changes, the third party must designate a new POC.
- All third-party access to High Security Systems must be approved by the Information Security Officer or their designee.
- Third parties may access only the systems that they support or maintain.
- All third-party accounts on High Security Systems will be disabled and inactive unless needed for support or maintenance. Requests for enabling access must follow the procedure outlined in The Loyola University Chicago Vendor Access to Internal Systems Policy. Requests for access outside of this policy are expressly denied. The server System Administrator will be responsible for enabling/disabling accounts and monitoring vendor access to said systems. All third parties with access to any High Security Systems must adhere to all regulations and governance standards associated with that data (e.g. PCI security requirements for cardholder data, FERPA requirements for student records, HIPAA requirements for Protected Health Information). Third party accounts must be immediately disabled after support or maintenance is complete.
- Data must not be copied from high security systems to a user's remote machine.
- Access will be disconnected automatically after 24 hours.
- Users will abide by the above user access guidelines.

Physical Access

All ITS data centers will abide by the following physical security requirements:

- Video surveillance will be installed to monitor access into and out of ITS data centers.
- Access to ITS data centers will be accomplished the use of electronic badge systems.
    - Only the Facilities Department, ITS Infrastructure Services Director, and the Network Services Team will have physical key access.
- Physical access to ITS data centers is limited to ITS personnel, designated approved Loyola employees or contractors whose job function or responsibilities require such physical access.
    - These individuals will be classified appropriately in the ITS Roles and Responsibilities Matrix.
- Loyola badges will be prominently displayed.
- Visitors accessing ITS data centers will be accompanied by authorized ITS personnel, and all access will be logged via the ITS Data Center Visitor Access Log.
    - This log will be stored at each ITS Data Center.
    - Each visitor, and accompanying authorized ITS personnel, must sign in and out of the data center.

- The log will be kept for at least a period of three months.

- Modification, additions, or deletions of physical access to ITS data centers will be accomplished by utilizing the ITS High Security Authorization Form.
- All terminated onsite personnel and expired visitor identification (such as ID badges)" will have their access revoked immediately.
- Physical access requires the approval of the ITS Infrastructure Services Director.
- The Information Security Team and the ITS Infrastructure Services Director will audit physical access to ITS data centers on an annual basis.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Institution, Management, Supervisors or Representatives	• Explain the terms of this policy to employees and students and assist users to understand the requirements of this policy • Ensure that all users follow the requirements of this policy
Jim Pardonek, Director and Chief Information Security Officer	• Enforcing the Access Control Policy at the University by setting the necessary requirements.
All users (Employees and contractors, Students, Visitors and/or Volunteers)	• Comply with the requirements of this policy • Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible

VI. Related Policies

Please see below for additional related policies:

- Security Policy
- Privileged Access Policy
- Vendor Access to Internal Systems Policy

Approval Authority:	ITESC	**Approval Date:**	April 19th, 2018
Review Authority:	Jim Pardonek	**Review Date:**	January 29th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu