Access Control Policy

Applies To:	All	Policy Number:	ITS-0035
Issued By:	AVP for IT	Policy Version Number:	1.0
Date Issued:	July 1, 2016	Last Review Date:	July 1, 2016
		Last Revised Date:	July 1, 2016

Scope
This policy applies to University faculty, staff, students, contractors and vendors that connect to servers, applications or network devices that contain or transmit Protected Data, per the Data Classification Policy. All servers, applications or network devices that contain, transmit or process Protected Data are considered "High Security Systems".

Purpose
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.

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 AVP for IT, with a valid business justification. Account creation, deletion, and modification as well as access to protected data and network resources is completed by the respective system custodian.

On an annual basis, the AVP for IT will audit all user and administrative access to High Security Systems. Discrepancies in access will be reported to the appropriate supervisor in the responsible unit, and remediated accordingly.

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 users will be disabled after 90 days of inactivity.
- Users will not login using generic, shared or service accounts.

Administrative Access

- Administrators will abide by the Privileged Access Policy.
- 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.
- 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 University of Detroit Mercy community. Use of this computer and network are subject to all applicable University policies, including Information Technology Services policies. 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 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 Virtual Private Network (VPN).
- Any third party, non-University 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 AVP for IT.
- Third parties may access only the systems that they support or maintain.

- All third party accounts on High Security Systems will be disabled and inactivated upon completion of work unless needed for support or maintenance. The server System Administrator will be responsible for enabling/disabling accounts and monitoring vendor access to 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).

- Data must not be copied from high security systems to a user's remote machine.

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 through the use of electronic badge systems.

- Physical access to ITS data centers is limited to ITS personnel with a business need for such access, designated approved University employees or contractors whose job function or responsibilities require such physical access.

- 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 twenty-four months.

- Modification, additions or deletions of physical access to ITS data centers must be approved by the AVP for IT.

- Physical access requires the approval of the AVP for IT or the Senior Network Manager.

- The AVP for IT will audit physical access to ITS data centers on an annual basis.

Policy adherence

Failure to follow this policy can result in disciplinary action as documented in the Acceptable Use & Security Policy.

History and Updates
July 1, 2016: Initial Policy