LOYOLA UNIVERSITY MARYLAND

— 1852 —

Datacenter Physical Access Policy

Purpose:

In order to support sound University-wide information security practices, compliance with various State and Federal legislation, and with various industry standards and best practices, this Datacenter Physical Access Policy ("Access Policy") applies to all employees of (direct or via contract), and organizations within the University.

The information resources entrusted to Loyola are among the University's most valuable assets, and must be managed in a manner that supports appropriate levels of information security, integrity, confidentiality, and availability for lawful educational and business purposes. The University's most sensitive data are stored within the two Datacenters (Knott Hall and Timonium), and in order to ensure both the security and availability of that data it is necessary to maintain strict controls over both access to and use of those rooms.

To that end, this Policy will define which members of the University have the need to access the Datacenters, how that access will be controlled, and will provide rules governing use of the Datacenters and conduct while within the Datacenters.

Principles:

The physical security and availability of critical University data assets are paramount to the function of the University. Therefore, this policy is designed in order to ensure that:

1. Control is maintained over which individuals have physical access to the Datacenters
2. The list of individuals with physical access is limited to as few people as possible
3. The Datacenters are used ONLY for their intended function, which is to house technology systems
4. Individuals with physical Datacenter access have a clear set of guidelines as to acceptable behavior while within the Datacenters

Scope:

1. This policy covers all access by any employee, contractor, student, or other person to either of the University Datacenters (presently Knott Hall 103 and Timonium 29).
2. This policy covers all use of either University Datacenter by any person with access.

Definitions:

1. Datacenter: Knott Hall Room 103, Timonium 29, and any future facility housing University data hardware.

2. Authorized Person: a direct employee of the University who has been granted access to the Datacenters due to the requirements of their position.
3. Visitor: Any person (whether a University employee or not) granted temporary access to either datacenter who is not on the permanent roster of Authorized Persons.

Policy:

Datacenter Access:

1. Any accessing of either Datacenter by any person not expressly permitted access is forbidden.
2. Access to either datacenter will be through two-factor authentication, requiring both a key card and a PIN input on a physical keypad on the card reader.
3. Public Safety will maintain a roster of Authorized Persons (consisting of only direct University employees) who are permitted access to the Datacenters. This roster will contain only individuals who have been approved by the Office of the CIO, and no one shall be granted access without this approval.
4. In order to request access to the Datacenter, an employee of the University shall have their supervisor submit a request, in writing, to the office of the CIO for approval. This written request shall contain:
    a. The person's name
    b. The person's position with or relationship to the University
    c. The person's Loyola ID number
    d. The name, position, and contact information of the individual requesting that this person be given access
    e. A description of the reason for requiring access
        i. What system they will be maintaining
        ii. The nature of that maintenance
        iii. The criticality of that maintenance
5. Criteria for Access: Additions to the list of Authorized Persons will be made only for the following reasons:
    a. The person's job position requires them to carry out maintenance of IT related (networking, servers, storage, etc) hardware or software which requires a physical presence in the Datacenter to complete.
    b. The person's job position requires them to carry out maintenance of Physical Plant resources (electrical, fire suppression, air conditioning, etc.) which requires a physical presence in the Datacenter to complete.
6. Upon approval by the Office of the CIO, Public Safety will add the employee to the roster of Authorized Persons, add the proper access to that person's card key, and issue that person a unique PIN for entry.

7. Twice per year, the department of Public Safety will provide to the Office of the CIO, in writing, a copy of the list of Authorized Persons.
8. Public Safety employees will maintain physical key access to the Datacenters for use in emergency situations.

Monitoring of Datacenters:

1. Public Safety will monitor all access to the Datacenters and will respond to attempts at unauthorized access as appropriate.
2. Public Safety will install cameras in the Datacenters in order to monitor access to the Datacenters and will record camera feeds for use in any needed investigations.
3. If unauthorized access is detected, Public Safety should notify the Technology Services Security Operations Center Director immediately so an incident can be opened and investigated.

Visitor Access:

1. Any individual on the permanent roster of Authorized Persons to access the Datacenters is also authorized to grant others temporary access to the Datacenters if this access is necessary for the business of the University. Inquiries from visitors (contractors, etc) requesting access to the Datacenters will be processed by the Office of the CIO.
2. All visitors shall be directly supervised by an authorized University employee who is on the list of Authorized Persons for the entire time while in either Datacenter.
3. Any Authorized Person who provides datacenter access to any Visitor shall be responsible for the actions of the Visitor while in the Datacenter.

Use of Datacenters:

1. University Datacenters exist for the express purpose of housing critical server, storage, and networking infrastructure equipment only.
2. Any other use of the Datacenters (i.e. for equipment storage, as general workrooms for non IT-related tasks, etc) is forbidden.
3. Persons who are permitted access to the Datacenters shall access and use them only as required in the course of their job duties.
4. Persons who are permitted access to the Datacenters shall exercise all due caution in the physical care of the equipment housed therein.
5. Persons who are permitted access to the Datacenters shall maintain them in an appropriate state of cleanliness and orderliness.

Penalties and Enforcement:

Enforcement of this policy will be in accordance with University policies;

Staff & Administrators Policy Handbook: Section 1.28 Discipline

Effective Date, Review and Revision of Policy:

This Security Policy will be effective as of the date of signature by the approving authority and will be subject to review and revision at least yearly and as updates are needed. In cases where immediate compliance with this policy is not reasonably feasible, a detailed plan must be developed for becoming compliant, and that compliance plan must be registered with and approved by the Office of the CIO.

Approvals:

Chief Information Officer:	*Louise Finn*	Date:	October 15, 2015
Director of Public Safety:	*Tim Fox*	Date:	October 15, 2015
Director of Facilities:	*Jennifer Wood*	Date:	October 15, 2015
Director of Event Services:	*Joe Bradley*	Date:	October 15, 2015