GA 39. Physical Security Policy

Title:	Physical Security policy
Policy Number:	GA 39/ 07.18
Effective Date:	July 24, 2018
Issuing Authority:	VP for Development

1. RATIONALE

This policy will establish physical security guidelines that apply to all computing and networking equipment locations. It is important to note that incremental degrees of security will be needed for each area depending on the actual equipment configuration and critical need to the institution.

2. POLICY

All areas will be classified into two categories:

- Office
- Restricted

Office areas are simply that, office locations for RHU IT/IS Department employees. These areas contain computing equipment and other data that should be protected at all times.

Restricted areas are those areas that belong to the RHU IT/IS Department and contain equipment owned and/or operated by the RHU IT/IS Department or a third-party vendor
such as:

- Switch closets
- Data Centers
- Videoconferencing rooms
- RHU Department storage areas

At minimum, all office and restricted locations require the following security mechanisms:

- Solid wood or steel door
- Either keyed handle or deadbolt lock

All RHU IT/IS Department restricted and office locations should contain the following recommended security mechanisms:

- Reinforced steel doors and frames
- Keyed deadbolt locks
- ID card access
- Steel bars over windows

3. RELATED DOCUMENTS

> IT Manual

4. APPROVAL AND REVIEW

OFFICER RESPONSIBLE: VP for Development

AUTHORITY: University Administrative Board
POLICY REVIEWED BY: VP for development, IT Department/ Infrastructure & Security

EFFECTIVE DATE: July 24, 2018

REVIEW DATE: As needed

REVISION HISTORY: None.

RELATED POLICIES: All University Policies and Procedures

FINAL APPROVAL BY THE PRESIDENT:

Signature:

Date: July 24, 2018