GA 31. Door Access Control System Policy

Title:	**Door Access Control System Policy and Procedure**
Policy Number:	GA 31/07.18
Effective Date:	July 24, 2018
Issuing Authority:	Office of the President

1. RATIONALE

RHU operates a door access control system to manage and facilitate access to space and equipment by authorized users (faculty/staff, students and affiliates) and in particular, and to safeguard members of RHU and its physical asset. IT CSS operates and manages the access control system at RHU.
Access Control System is an electronic access technology that allows users to use the current magnetic ID card as the means of access. It replaces traditional keys with an electronic door strike that is hard wired and networked into the current Information Technology infrastructure to allow for remote communication. The electronic access readers can be horizontally or vertically swiped.

2. Policy

The safety and security of the University's physical space and assets is a shared responsibility of all members of the University community. To meet this obligation, the University has established Access Control policy provisions to address the administration and management of Access Control systems and measures to ensure their integrity. Access Control privileges are determined and assigned by University administrators based on the specific needs and requirements of the University and the key/card holder.

Total Access Keys
Any keycard that opens all doors with access control system on the RHU campus. Total Access Keys are only distributed to the following:

1. President
2. Vice Presidents
3. Access Control System Administrator/s

Office Master Keys
Any electronic card that opens multiple doors within a specific office suite or department space on RHU campus. Office Master Keys are only distributed specific personnel as requested by the department head and after the approval of the concerned administrator/s.

Access Control Approval Process – Levels of Approval

Access is granted to staff and faculty members to their assigned work premises such as offices, classrooms, labs as per the allocation directories collected from the concerned department/s.

Every further access requests must be made through an approval channel. There will be three (3) levels of approval that any request can fall under. The level of Access Control approval for any area is determined by the level of risk and exposure. The following levels of approval will apply to all access requests:

Level 1 – Single or Multiple doors within a department within normal business hours requires approval from the direct supervisor and/or department head.

Level 2 – Single or Multiple doors within a department outside normal business hours requires approval from the direct supervisor and department head.
Level 3 – Single or Multiple doors access in another department within or outside normal business hours requires the approval of the requester's department head, the head of the department having authority on that subject door and the concerned Vice President/s.

New Employees/ New Faculty

If full-time employees/faculty or part-time employees/faculty is new to RHU campus, employee's department or HR liaison will process all necessary information through the HR system in order for new employee to obtain the Access Control Card/ID Card.
It is the responsibility of the card key requester or the liaison in his/her department to collect the keycards from the issuing department.

Transfer of Employee/Faculty
If an employee/faculty is transferring to a new work premises or department within RHU campus, the following procedure must be applied:

1. Employee's current department liaison must submit a request to deactivate that employee's access.
2. Employee's new department liaison will then request the activation of the employee's new location.

Access Control Policy Violations
The following acts are examples of violations of the key policy:

- Loaning key card
- Transfer of key cards without authorization
- Altering key cards, locks or mechanisms, installation of padlocks on University spaces (i.e. offices, labs,
etc...)
- Damaging, tampering or vandalizing any University lock or hardware
- Propping doors open
- Admitting unauthorized person/s into the a location
- Failure to return a key when requested by the department head, administration, the issuing department, or upon leaving the employment of the University.

- Failure to report missing keycard/s

3. STAKEHOLDER IMPACT AND SCOPE

It is the responsibility of each RHU student and staff member to familiarize themselves with policies and procedures relevant to their area of work, and execute their responsibilities in reviewing petitions and completing forms accordingly.

4. RELATED DOCUMENTS

IT Manual

5. APPROVAL AND REVIEW

OFFICER RESPONSIBLE: VP for Development and Information Technology

AUTHORITY: University Administrative Board

POLICY REVIEWED BY: VP for Development and Information Technology, Client Support and Services Supervisor

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: