GA 25. Information and Computer Resources Use Policy

Title:	**Information and Computer Resources Use Policy**
Policy Number:	GA 25/07.18
Effective Date:	July 24, 2018
Issuing Authority:	Office of the President

1. RATIONALE

The primary purpose of the university information and computer resources is to better serve the administrative, teaching, studying, and research of the university community. The use of information and computer resources is permitted by RHU for bona fide purposes only, i.e., work, teaching, study, research, or related activities. The University information and computer resources shall only be accessed by authorized users for work or academic-related activities.

2. Policy

Persons authorized to access the university information or computer resources shall not disclose confidential information to unauthorized persons and shall not use the University resources for personal gain or in any manner that may be prejudicial to the interests of the University.

Persons having access to university information and/or the University's computer resources shall sign an acknowledgment that they have read, understand, and will abide by this policy relating to the use and misuse of the university information and computer resources.

Definitions

***Information Resources*:** under this policy, include all RHU information, materials, know-how, and data, whether oral, written, digital, or graphical, disclosed, accessed, provided, or otherwise known.

***Computer resources*:** include, and are not limited to, digital storage media, computers and networks owned or operated by the University or to which the University is connected and any data contained therein.

Regulations

1. Each RHU information and computer resources user is considered as responsible for the security of the resources, confidentiality, password maintenance, and file protection measures.
2. It is the responsibility of the employee/student supervisor to retrieve all entrusted data and information and revoke the system access and authorization upon severance of the relationship for any reason whatsoever. The two above conditions should be confirmed on the clearance checklist where applicable.
3. Users of RHU information and computer resources are accountable for any action (or inaction) undertaken or facilitated by them or under their direction or with their knowledge, or which they should have known or detected, including improper paper/electronic transactions, misuse of resources, or unauthorized access and use of resources.
4. The misuse of resources includes, but is not limited to:

    a) Damaging or altering records or programs, furnishing false or forged information/passwords, invading the privacy of another user by using passwords, files, programs, or data without permission.

b) Unauthorized use of university information, computer hardware, software, accounts, or passwords.

c) Deliberate damage or impairment of university resources or interference or impairment to the activities of others.

d) Unauthorized copying of university information or downloading of university data resources.

e) Unauthorized activities (commercial, political, etc.) involving the use of University information or computer resources.

f) Intellectual property infringements.

g) Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the primary users' explicit permission.

h) Revealing confidential information or information that could be detrimental to the University.

5. No RHU information or computer resources user, employee, or student is allowed to maliciously access, alter, delete, damage, or destroy any system, network, program, or information that is considered university property.
6. It is the obligation of every RHU information computer resources user who has knowledge of improper electronic transactions, misuse of resources, or unauthorized access and use of resources to immediately report such occurrences to the University authorities.
7. The pre-disposal data sanitization of RHU's hardware and storage media to protect the intellectual property of RHU and the confidentiality of personal information is the responsibility of the data steward/owner. The data steward should consult with the IT Department prior to disposing of any computer equipment or storage media. IT Department will provide an approved sanitization tool and provide assistance in properly sanitizing the hardware or storage media. IT Department will provide a certification that the equipment or media has been properly sanitized before it can be transferred to another user/department, recycled, donated, sold, or disposed of as scrap.

Violations

Violation of any of the above, and based upon the severity of the incident, may result in disciplinary action up to and including suspension, termination of employment, or expulsion from the University and in legal, including criminal, proceedings.

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: