3.480 RCUH Electronic Communications

I. Policy

This policy governs the proper use of electronic communications media/services belonging to the respective programs in which an RCUH employee is employed. Electronic media/services provided by the project are considered the "property of the project." As such, the primary purpose of their use should be to facilitate and support the business of the project.

In addition to this policy, employees may also be subject to additional related policies enforced by the project, institution, or governmental agency.

Employees who violate this policy or additional related policies enforced by the project may be subject to disciplinary action, up to and including termination of employment.

II. Responsibilities

A. RCUH Employee

1. Read and sign the Confidentiality Requirements for Personal Identifiable Information Acknowledgment Form to signify understanding of responsibilities under this policy.
2. Understand that electronic communications media/systems are the property of the project, and there is no entitlement to privacy.
3. Comply with the provisions of this policy. Violations may results in disciplinary action, including termination.
4. Employees are responsible for keeping their login and password information confidential, safe, and secure.
5. Upon resignation or termination of employment, or at any time upon request, produce the electronic equipment for return or inspection.
6. Report any violation of this policy immediately to the RCUH Director of Human Resources.

B. Principal Investigator

1. Ensure project personnel understand and comply with this policy. Enforce the provisions of this policy.
2. Report any violation of this policy immediately to the RCUH Director of Human Resources.

III. Applications

RCUH employees working for University of Hawai'i (UH) projects are subject to Information Technology Policies and Procedures applicable to their respective University, College, Institute or other applicable UH entity.

RCUH employees working for non-University of Hawai'i projects are subject to information technology policies and procedures of that business entity.

In the absence of any policy, this policy shall apply to all RCUH employees who, in the course of their employment, have access to electronic communications media services, systems, and/or equipment.

This policy applies to all Principal Investigators and/or designees who employ individuals through the RCUH.

Any non-RCUH employee found to be participating in inappropriate activities described in this policy may be reported to his/her respective employer/institution.

IV. Details of Policy

A. Definition of Electronic Communications Media/Services

Electronic Communications Media/Services Include the Following – Electronic communications media/services include but are not limited to program systems and network, servers and workstations, laptops, personal electronic communication devices, email, phones, voicemail, fax machines, external electronic bulletin boards, online services, the Internet, and other forms of electronic communication technologies used for project business.

B. Situations When This Policy Applies – Electronic communications media/services are all electronic communication media/services that are

1. Accessed on or from work premises or at other locations where work may be performed;
2. Accessed using project computer equipment or via project-paid access methods (i.e., Verizon Wireless, AT&T, etc.);
3. Used in a manner that identifies the individual with the project.

C. Ownership of Electronic Communications and Rights to Privacy

1. Electronic Communications Media/Systems Are the Property of the Project: All equipment, messages, data files, and programs stored in or transmitted via the electronic communications media/systems **are the property of the respective program**. This includes all information and data processed, transmitted, received, and stored on project equipment/systems.
2. Access to Electronic Communications Media/Systems**:** Electronic communications media/systems may be monitored by the Principal Investigator/designee or the RCUH at any time to the extent necessary to ensure electronic communications media/services are being used in compliance with the law, this policy, and other policies. If applicable, the Principal Investigator and/or

the RCUH may disclose any of its electronic communication, equipment, or systems to law enforcement or other third parties without prior consent of the user.

3. No Employee Rights to Privacy: There are no rights to privacy under this policy. Employees should not assume electronic communications are totally private. Therefore, if an employee has sensitive communications or information to transmit, they should use other means.

D. Personal Use of Project's Electronic Communication Media/Systems

1. Electronic communications media/services are provided for business purposes. Limited, occasional, or incidental use of electronic communications media/systems (sending/receiving) for personal, non-business purposes is understandable and acceptable. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege. Failing to do so will result in a loss of this privilege and possible disciplinary action.
2. Employees are not authorized for personal use of electronic systems that result in expenses or charges to the project. If additional charges are incurred as a result of personal use, the employee will be responsible for those charges.
3. Employees should exercise caution while using public computers and networks, especially for storing and/or accessing their login, password, and/or other sensitive information.

E. Prohibited Communications or Use of Electronic Communications Media/Systems

1. Electronic communications cannot be used for knowingly transmitting, retrieving, or storing any communication that is
   a. Discriminatory or harassing;
   b. Derogatory to any individual or group;
   c. Obscene;
   d. Defamatory or threatening; or
   e. Engaged in for any purpose that is illegal, disruptive, or contrary to the RCUH policy or business interests, or for any other uses that violate RCUH or project policies and guidelines.
2. Employees are also strictly prohibited from engaging in, or attempting to engage in, any of the following activities:
   a. Monitoring or intercepting the files or electronic communications of other employees or third parties
   b. Using electronic communication equipment or software for outside business activities or unauthorized non-business purposes
   c. Personal use of equipment that would compromise the security or integrity of the project
   d. Hacking or obtaining access to systems or accounts they are not authorized to use

e. Breaching, testing, or monitoring computer or network security measures

f. Compromising system or network security or performance within the network, or any connected network or system

g. Removing any electronic system/equipment, attached peripherals, supplies, or documentation without the expressed consent of the Principal Investigator

h. Sending email or other electronic communications that attempt to hide the identity of the sender or representing the sender as someone else

i. Using electronic communications media/services in a manner to cause network congestion or significantly hamper the ability of other people to access and use the system

j. Accessing or signing onto electronic communication media/services using someone else's login information. An identification code shall be used only by the person to whom it is assigned, and that individual is also responsible for maintaining the confidentiality of the password. Therefore, login information must not be shared with anyone else, unless directed by the Principal Investigator and/or RCUH Director of Human Resources.

F. **Confidentiality of Electronic Communications Media/Systems** – Employees must respect the confidential and proprietary information of others. Employees are prohibited from copying, sending, receiving, and distributing copyrighted material (i.e., software, database files, documentation, or articles using email or other forms of electronic communications media/services) unless authorized by license agreements.

G. **Use of Encryption on Electronic Communications Media/Systems** – Employees can use only encryption software supplied by the original software vendor or by the project's institutional parent organization. Employees who use encryption on files stored on a company computer must provide their Principal Investigator or designee with a sealed envelope containing a hard copy record of all passwords and/or encryption keys necessary to access the files.

H. **Employees Must Protect Project Electronic Communication Media/Systems** – Employees must take every precaution necessary to protect project electronic communications media/systems and equipment from loss, damage, or theft, especially when such equipment is easily portable (i.e., laptop, cellular phone).

I. **Safety Issues for Cellular Phone and PDA Use** – Employees whose job responsibilities include regular or occasional driving and who are issued a cell phone or electronic communication device for business use are expected to refrain from using their phone while driving. Safety and legality come before all other concerns. Traffic violations and related liabilities resulting from the use of the project phone or PDA while driving will be the responsibility of the employee.

J. **Access to Electronic Communications Media/Systems May Be Restricted to Employees**

1. Access or Use of Electronic Communications Media/Systems May Be Restricted to Employees: At the Principal Investigator's discretion, access may be restricted

or rescinded if there is a substantiated reason to believe that violations of law or policy have taken place, or when it is believed that continued access could result in destruction of information.

2. Login Information May Be Revoked or Be Required to Be Disclosed: The Principal Investigator/designee and the RCUH reserves the right, without advance notice, to revoke access, override user's passwords, or require users to disclose passwords and/or codes to facilitate access to information that is processed and stored on the electronic systems.
3. Access Will Be Restricted for Employees Placed on Disciplinary Status: If an employee is placed on disciplinary status (e.g., placed on suspension pending termination or under investigation), access may be restricted or removed without notice. Employees will be required to surrender all access and electronic devices during any disciplinary action.

K. **Use of a Notice and Consent Banner** – All of the conditions listed in this policy will apply regardless of whether the access or use of an information system includes the display of a notice and consent banner. When a banner is used, the banner functions as a reminder of the conditions that are set forth in this policy, regardless of whether the banner describes these conditions in full detail.

V. Procedures

A. **Employees Must Sign Acknowledgment Form** – Upon hire, new hires must read and sign the Confidentiality Requirements for Personal Identifiable Information Acknowledgment Form to signify their understanding of their responsibilities under this policy.

B. **Procedures for Reporting Violations of This Policy** – Any violations of this policy may be reported to the Principal Investigator or authorized designee, or to the RCUH Director of Human Resources.

VI. Contact

Nelson Sakamoto, Director of Human Resources: (808) 956-6965
nsakamoto@rcuh.com

VII. Relevant Documents

Confidentiality Requirements for Personal Identifiable Information Acknowledgment Form

Date Revised: 03/17/2011, 04/21/2017, 08/08/2017