EMPLOYEE COMPUTER USAGE

Section: Information Technology

Policy: In order to carry out job responsibilities, staff may be individually assigned a computer system or may share a computer system. Department-provided computer systems should only be used for work purposes. All department staff members are expected to understand and follow University of Georgia (UGA) computer usage policies.

Purpose: The purpose of this policy is to outline expectations for all staff members using department computer systems as a part of their position responsibilities.

Scope: This policy applies to all University Housing staff members requiring computer access.

Background: To better protect students, staff, and information technology resources within University Housing.

Procedure:

I. The University Housing Human Resources (HR) staff is responsible for notifying the Information Technology (IT) staff via IT request when an employee has been hired, transferred, resigned or separated. IT staff will grant or remove access to the applicable systems in accordance with the request instructions or established University protocol.

II. For employees needing access to some systems, such as StarRez and Banner, Family Education Rights and Privacy Act (FERPA) training is required prior to access being provided. The policy and procedures for staff access for StarRez can be found at https://housing.uga.edu/sa_docs/staff/policies_it_starrezaccess.pdf and Banner at https://housing.uga.edu/sa_docs/staff/policies_it_banneraccess.pdf.

III. Upon beginning a new position in University Housing, all employees who will have responsibilities working on a departmental computer system, must read and be expected to understand the applicable UGA policies, standards and guidelines published by the Office of Information Security. These policies, standards and guidelines can be found at https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/. Staff must also complete a biannual cybersecurity training, as required by the University System of Georgia.

IV. Every employee will be provided their own user ID and password to access appropriate systems. Although not required, staff members are strongly encouraged to change their passwords periodically. Employees shall not share passwords for any reason.

V. All employees are expected to lock their computers when leaving the immediate area where the computer is installed. This can be achieved by executing one of the following actions on Windows machines: Simultaneously press the Windows+L keys, or simultaneously pressing the Ctlr+Alt+Del keys and selecting Lock from the pop-up menu, or by pressing the Windows button then selecting the user icon and choosing Lock. All windows computers have been configured to automatically lock after 20 minutes of inactivity. When ready to resume computer use, press any key on the keyboard and use your MyID and password to regain computer access.

VI. All employees must power off the computer at the end of the workday, unless instructed by IT staff for a one-time case to leave the computer powered on.

VII. All employees are responsible for backing up their work data, such as documents and photos to the shared drive or OneDrive.

VIII. After a computer upgrade or exchange, the IT staff will maintain the computer's disk drive unchanged for 14 days. The disk drive will be formatted (all data erased) after 14 days.

IX. It is the supervisor's responsibility to oversee student, temporary or part-time staff appropriate use of the computer system.

X. The IT staff will notify the staff member's supervisor and appropriate management team member should any inappropriate computer usage be incidentally discovered.

Revised: Sept. 25, 2023
Revised and approved by management team: Dec. 7, 2021
Revised: Dec. 13, 2019
Revised and approved by management team: April 2, 2019
Revised: Feb. 7, 2018
Revised: February 2016