Policy Title:	Report Loss or Theft of CCU-owned Equipment
Policy Number:	UNIV-490
Revision Date:	October 2020
Policies Superseded:	None
Policy Management Area(s):	Information Technology Services

SUMMARY:

Coastal Carolina University (CCU) issues various equipment types to faculty and staff in support of its business operation and mission. Equipment may include but is not limited to computers and laptops, tablets, iPads, cell phones, and associated device peripherals. This policy addresses the equipment's user responsibility and procedures of reporting loss or theft of CCU-owned equipment.

POLICY:

I. Any employee that is the assigned custodian of a University-owned equipment that is lost or stolen is responsible for following the reporting procedure.

II. If your CCU-owned device has been lost or stolen:

   A. If the device was lost or stolen off-campus, immediately file a police report with the local police department.

   B. Regardless of whether the device was lost or stolen off campus, you are required to contact and file a report with the CCU Department of Public Safety by calling 843-349-2177. This may be in addition to the police report filed with the local police department.

   C. If the device contained or had access to any CCU information, applications or data, including but not limited to email and/or grades, contact the CCU Office of Information Technology Services (ITS) at 843-349-5000.

   D. Notify your supervisor of the loss or theft.

III. ITS will update their asset records and check the status of the device to locate, recover, or render the device inoperative. ITS will reset user passwords associated with the device

and block access to network resources. Users will then be required to change their passwords and any other applicable login credentials to regain access to the CCU network.

IV. The ITS information security manager will review and investigate all reported lost or stolen devices to determine potential data loss. If there was a potential compromise of sensitive information or exposure of network resources, the information security manager will confer with appropriate CCU officials and legal counsel, coordinate notification of affected individuals, and report the incident to state or federal agencies as required.

V. User Security Precautions

When using a CCU-owned device (e.g., laptop, cell phone, iPad, or other) or a personally owned device to access CCU's network, or when storing files with sensitive CCU data on any device, take the following precautions:

A. Do not leave devices unattended in a public area or visible in a parked car even "for a moment."

B. Utilize a login password for the device.

C. Store sensitive CCU data, as much as possible, only on approved CCU network storage drives rather than on mobile devices or laptops, and access the data using CCU's virtual private network (VPN) access.

VI. Related policy links include, but are not limited to:

General Usage – Network and Computing

Data Privacy, Classification, and Protection