UCONN

Administrative Policy
2008-03 Mobile Computing Device Security

Title	Mobile Computing Device Security
Policy Owner and Contact Information	Information Technology Security itsecurity@uchc.edu / UConn Health Service Desk 860-679-4400
Applies to	All UConn Health workforce members, including employees, faculty, staff, students, residents, volunteers and other individuals.
Campus Applicability	UConn Health
Effective Date	5/15/20

PURPOSE:

To establish requirements for the secure connection and deployment of mobile computing and removable storage devices within UConn Health to support both privacy and security of sensitive information and compliance with applicable agency and regulatory requirements.

APPLIES TO:

This policy applies to all UConn Health workforce members, including employees, faculty, staff, students, residents, as well as volunteers and other individuals with approved access to UConn Health systems.

DEFINITIONS:

Mobile Computing Devices (MCD) includes, telecommunication and portable computing devices which can execute programs or store data, including but not limited to laptops, tablet computers, smartphones, and external storage devices.

POLICY STATEMENT:

UConn Health data may be stored or processed on a MCD, excluding personally owned storage devices, if ALL of the criteria below are met:

1. UConn Health Mobile Device Management technology is configured on the device.
2. The device stores only the minimum data necessary to perform the function necessitating storage on the device.
3. Information is stored only for the time needed to perform the function.
4. The device requires a password for access and is encrypted using methods authorized by the UConn Health Information Technology (IT) department.
5. The device is configured to allow UConn Health the ability to initiate a remote “wipe” or deletion of data if a credible report is received that the device is lost or stolen.

UConn Health Confidential data is not permitted to be *stored* on personally owned laptops or external storage devices, including but not limited to USB drives, external hard drives, etc.

All MCD equipment procured by and/or funded by UConn Health is institutional property, regardless of the source of funds from which they were purchased.

Users may not bypass or disable UConn Health required security mechanisms.

Devices configured to bypass vendor security controls are not permitted to access UConn Health IT resources.

PROCEDURES/FORMS:
The user understands and agrees that such *access* is considered a personal convenience for the user and as such, UConn Health will not reimburse or otherwise compensate the user for any costs associated with such access.

User agrees to secure their MCD(s) using software and/or security controls as defined by UConn Health, including but not limited to up-to-date anti-virus software and vendor released security patches.

The user understands that he/she may be held liable for any criminal and/or civil penalties that may result from loss, theft or misuse of the confidential information accessed and/or stored on the personal device.

Upon termination of affiliation with UConn Health, users agree:

1. To immediately delete all institutional data stored on the device, excluding research data which will move with the MCD owner.
2. To remove the UConn Health email account and WiFi settings from the device.

Users acknowledge that UConn Health does not provide support for personally-owned devices and has no liability for such devices. Configuration of any personally owned device is the user's responsibility.

Failure to complete the above may result in the device being auto-wiped by IT Security.

Users are expected to take appropriate precautions to safeguard their MCD against loss or theft. Unauthorized physical access, tampering, loss or theft of a MCD must be immediately reported to UConn Health Public Safety.

REFERENCES:
None

RELATED POLICIES:
2002-43 Confidentiality

ENFORCEMENT:
Violations of this policy or associated procedures may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, the University of Connecticut Student Code, other applicable University Policies, or as outlined in any procedures document related to this policy.

APPROVAL:

Andrew Agwunobi (Signed) May 22, 2020
UConn Health Chief Executive Officer

Kiki Nissen (Signed) May 22, 2020
Administrative Policy Committee Co-Chair

Janel Simpson (Signed) May 21, 2020
Administrative Policy Committee Co-Chair

New Policy Approved: 4/14/2003
Revisions: 5/27/2008, 7/10/2012, 3/12/2013, 2/17/2015, 5/15/20
Replaces: Policy #2003-32 Portable Computing Device Security (4/14/03)