ITS Support Addendum for Teleworking
08.112

Authority: CIO

History: Revised August 24, 2020; Revised March 18, 2020; Revised January 9, 2007

Source(s) of Authority: Office of State Human Resources Manual, Teleworking Program

Responsible Office: Information Technology Services

I. Applicability

This addendum applies to any university employee approved to telework under UNCW Policy 08.112 SHRA and EHRA Non-Faculty Teleworking Policy and Procedures. For this addendum the term "computing equipment" is any device that can store, process or transmit university data, such as, but not limited to, a PC, laptop, tablet, smart phone, etc.

II. Purpose

The information contained within this document outlines Information Technology Services (ITS) support and requirements for UNCW Policy 08.112

III. General

The highest standard of care must be taken by the teleworker to safeguard the confidentiality, integrity and availability of UNCW's sensitive information that is processed, transmitted or stored. Teleworkers must also ensure they adhere to the provisions set forth in the UNCW ITS policies. These policies can be accessed online at https://uncw.edu/policies/it/.

Computing equipment to be used by the teleworker may be provided by their respective departments documented in the Teleworking and Flexible Work Schedule Agreement Form.
University owned resources are preferable as they are configured to meet university security standards. Home networks must use strong data protection and the default credentials must be changed to a strong password. Home computers must use vendor supported operating system versions updated to the latest patches for the system and software, as well as provide virus and malware protection at a minimum. The teleworker must also ensure that critical or otherwise sensitive information, including physical documents, are protected from unintended disclosure, alteration, or destruction.

Teleworkers can receive technical support for their university owned computing equipment by contacting the Technical Assistance Center (TAC) at (910) 962-4357 during normal university business hours. In person, off campus technical support is not available. Further information regarding technical support can be found online at https://uncw.edu/itsd/help/

IV. Reporting Lost or Stolen UNCW Property or Data

A. Take the following actions in the event UNCW **property** is lost or stolen.
   1. Contact UNCW police
   2. Contact supervisor

B. For purposes of this Addendum, a data breach is defined as any protected information that is disclosed to an unauthorized source. In the event UNCW **data** may have been breached, contact UNCW ITS Information Security at itsecurity@uncw.edu.

V. Teleworker Requirements

Since teleworkers will not be protected by some of the security controls delivered on-campus, such as our firewalls and browsing protection, they must maintain good security practices when working remotely.

1. Always keep all university owned and personal computing equipment secured.
2. Sensitive data must be maintained on UNCW systems or in UNCW services such as SharePoint or OneDrive and be accessed remotely. (see #5)
3. To maintain separation of UNCW data and personal devices, do not store, process, or transmit data outside of official UNCW cloud services. (see #5)
4. Encrypt any sensitive data that is taken off campus on any type of storage device or media.
5. Approved methods to access UNCW Systems can be found at: https://uncw.edu/itsd/help/workingremotely.html
6. Ensure the security and configuration of all devices; including but not limited to current patch levels, effective anti-malware and virus protection, and appropriate network security controls.
7. For university owned computing equipment, do not alter ITS security configuration.
8. Ensure all connections, both data and telecommunications, are secure. Avoid using open or public (unencrypted) Wi-Fi for University business. For additional resources on using open or public Wi-Fi: https://uncw.edu/techtalk/2017/10/ask-an-expert.html.
9. Never provide your password to anyone or share your account access.
10. Use your UNCW email account or the UNCW Teams application for business communication - do not use your personal accounts for university business communication.
11. Only the teleworker is authorized to use university owned computing equipment.
12. Watch your email for TAC phishing alerts & security communications. *Stay vigilant for phishing or malicious attacks.* Please slow down and be mindful before you click on a hyperlink.
13. Immediately report the loss of university owned computing equipment or data breach as outlined above.
14. If you see anything suspicious, please email itsecurity@uncw.edu so that we can give your report immediate attention.
15. Please send any suspected phishing emails to phishing@uncw.edu.
16. For anything else, please contact the TAC or itsecurity@uncw.edu.
17. When the teleworker's relationship with UNCW is terminated, he or she shall be denied further access to university information technology resources, including retrieving personal information on state-owned devices.
18. Failure to comply with the requirements outlined in this ITS Support Addendum for Teleworking by the teleworker may result in a discontinuation of the teleworking assignment and may also result in disciplinary action up to and including termination.

VI. Department Responsibilities:

1. Maintain a record of the issued computing equipment.
2. Immediately report the loss of university owned computing equipment to UNCW Police or Breach of Data to ITS Information Security.