Enterprise Technology & Standards Security Standards for Teleworking/Remote Working

Please read the following procedures to ensure you understand the University of New Hampshire's cybersecurity standards, then sign to indicate that you have read, understand and will adhere to these best practices.

1. I will follow good cybersecurity practices as outlined here (https://td.unh.edu/TDClient/60/Portal/KB/ArticleDet?ID=1404)
2. I will use University-issued equipment whenever possible (i.e. University laptops).
3. It is my responsibility to ensure that the equipment I use for teleworking meets all ET&S security requirements to include:
    a) Configure all equipment in accordance with the UNH Computer Prep.
    b) Encrypt all media (i.e. internal hard drives, external hard drives, flash drives).
    c) Enable all security features on equipment (i.e. passwords, screen locks, remote wipe).
    d) Enable all automatic operating system, application security and malware protection updates
4. If I am unable to accomplish these security measures independently, ET&S can assist me. (Visit ET&S Desktop Management or call 862-4242). Customary service fees apply.
5. I will not share University-issued equipment (i.e. with other family members).
6. I will protect equipment from theft when not in use.
7. I will protect all printed material from unauthorized access.
8. I will log into the **UNH VPN** (*Pulse Secure*) prior to logging into University systems remotely.
9. I will store all University information on University servers whenever possible. If not possible, temporary storage of non-restricted data on password protected and encrypted mobile devices (i.e. laptop, jump drive) are permissible with prior supervisor approval. Storage of restricted[1] data on computers, external media and mobile devices must be approved in advance by ET&S Cybersecurity & Networking to ensure appropriate protections will be implemented.
10. I will not use public computers to log into University systems that contain restricted information (i.e. Banner) or access these resources over public networks, and will not use passwords used for restricted environments on public machines or for other purposes.
11. I will familiarize myself with phishing and vulnerability alerts provided by ET&S Cybersecurity & Networking and obtain training from CS&N if unclear about these standards.
12. I will review the UNH Technology & Cybersecurity Policy information at: https://www.unh.edu/it/cybersecurity-networking/cybersecurity-policies-standards-and-procedures
13. I will report all suspected compromises of computers or applications, including suspected breaches, immediately by calling 862-4242.
14. I will review Cybersecurity & Networking training materials and this policy at least annually.
15. My supervisor and I will verify my equipment's configuration is secure to current ET&S cybersecurity standards at least annually.

Employee Signature	Date Click here to enter a date.
Department Click here to enter text.	
Supervisor Name (PRINT) Click here to enter text.	

(*PLEASE PRINT DOCUMENT, SIGN AND ATTA*CH TO EMPLOYEE FLEX WORK PROPOSAL)

[1] http://www.usnh.edu/policy/usy/vi-property-policies/f-operation-and-maintenance-property#usyvif6