The University of Vermont

INFORMATION SECURITY, PRIVACY & CONFIDENTIALITY AGREEMENT

OFFICE OF AUDIT, COMPLIANCE & PRIVACY SERVICESuvm.edu/compliance/privacy-program

DO NOT FILL OUT THIS PDF FOR eTELEWORK.

YOU WILL BE PROMPTED TO FILL THIS OUT ONLINE WHEN YOU SUBMIT YOUR eTELEWORK REQUEST. THE LINK FOR eTELEWORK CAN BE FOUND HERE.

THIS FORM CAN BE USED FOR ALL OTHER PURPOSES.

By signing below, you are acknowledging that you have read this agreement and understand the general principles of maintaining the privacy, security and confidentiality of protected data. If you have any questions regarding allowable access or this agreement, discuss this with your manager, supervisor. If you have questions related to UVM's privacy program, contact privacy@uvm.edu. Questions related to information security should be directed to iso@uvm.edu.

EMPLOYEE INFORMATION

Employee Name		**Employee ID No.:**	
Department:		**Position No.:**	

<continued>

GENERAL CONFIDENTIALITY AGREEMENT

EMPLOYEE INITIALS

1. I acknowledge that:

   a. my job duties require that I access, use, and/or disclose sensitive, confidential, regulated, personally or other individually identifiable information most of which is protected under federal, state, international laws or under university policy (herein referred to as Non-Public Protected Data or "NPPD"). This may include personnel information, health information, transcripts, applications, demographic information, financial information, social security numbers, research data, controlled unclassified information (CUI), grades, or information pertinent to physical or virtual security (for example, residence locations, locations of equipment or dangerous materials, security staffing/scheduling data), and/or

   b. I have been issued a UVM owned or managed device.

2. I acknowledge that I have both a legal and ethical responsibility to protect the privacy, security, and confidentiality of NPPD.

3. I acknowledge that any unauthorized access, use, or disclosure of NPPD is strictly prohibited.

4. I acknowledge that my login credentials (username and password) are assigned to me and me alone and sharing my credentials with anyone else is prohibited. I further acknowledge that I may be held personally responsible for any activity that occurs under my login credentials.

5. I understand that, while I may be asked to enter my password for reasons such as tech support, I will never be asked to disclose my password to someone else to enter on my behalf. It is especially important that I never provide my username or password in response to an email, text or telephone request. I recognize that phishing or other communications designed to trick me into disclosing my credentials can look very real. I agree to verify that the communication is legitimate prior to entering my credentials. I further agree to notify UVM Information Security Office at iso@uvm.edu if I am unable to determine the legitimacy of the communication.

<continued>

6. I understand that I am only authorized to access that NPPD which is necessary for me to perform my job ("need-to-know"). I understand that not all data access can be controlled by technology settings and that my login credentials may provide access to NPPD that is not necessary to perform my job duties. As such, it is my responsibility to limit my own access to only that NPPD which is necessary for me to perform my job duties. □

7. I recognize that installing unauthorized software, applications or other programs could compromise the security of the information systems. As such, I acknowledge that I will only do so in compliance with UVM's policies and procedures. □

8. I understand that software needs to be kept up to date and that failure to do so creates security risks. □

9. I acknowledge that I am prohibited from performing system functions outside the scope of my job responsibilities. Unless I have been given express permission, tasks such as altering system functionality, adding users, and changing user access levels is strictly prohibited. □

10. I acknowledge that I have read the University policies and procedures related to my access and that I have been given the opportunity to ask questions. These policies include: FERPA Rights Disclosure, Computer, Communication, and Network Technologies Acceptable Use Policy, Information Security Policy, Information Security Procedures and Privacy Policy □

11. I acknowledge that downloading, extracting, copying, storing, or printing NPPD outside the scope of my job duties is prohibited. I understand that this includes, but is not limited to, saving information to a hard drive (internal or external), tablet, USB, smartphone or other device whether UVM-owned or personally owned unless I am specifically authorized to do so as part of my job duties. □

12. Even if I don't have access to the electronic systems, I may have access to other forms of NPPD (primarily paper or verbal). I understand that I am obligated to keep NPPD private and secure regardless of the format that the information takes. □

<continued>

TELECOMMUTING AND TECHNOLOGY

	EMPLOYEE INITIALS
13. I acknowledge that accessing or using NPPD while working remotely carries additional responsibilities.	
14. I will not manually download or save files containing high-risk NPPD* to my personal or non-UVM issued device. Data owners may, at their discretion, prohibit me from downloading low or moderate risk NPPD. Downloading non-sensitive, non-regulated and/or non-personally identifiable research data is not prohibited by this section unless the data owner has instructed me otherwise. ******High-risk NPPD*** *includes regulated data such as Protected Health Information (PHI), Controlled Unclassified Information (CUI), Non-Public Information (NPI). It includes protected data elements such as Social Security Numbers (SSNs), financial account numbers, passwords and government issued identification numbers. It also includes research data covered under explicit Data Use Agreements (DUAs) or award agreements and data that contains trade secrets or has any intellectual property concerns.*	
15. If using a personal device (i.e., smartphone, tablet, thumb drive, CD, external hard-drive or any other storage device), I will enable device security such as password protection, auto-lock and encryption.	
16. I will not save NPPD to my hard drive. All NPPD must be saved to an officially supported UVM service. Accessing UVM's centrally managed services, including servers, remotely may require use of the VPN.	
17. I acknowledge that any technology equipment issued to me such as laptops, desktops, printers, software, monitors, and other services such as fax lines are provided on loan by the University and remain the property of the University while they are on loan. All UVM issued equipment must be returned upon termination or upon the end date of my telecommuting agreement.	
18. I understand that access to data and information stored on UVM-issued or managed devices may be approved in accordance with university policies. Policies are designed to only allow access when needed while also supporting the university's mission. Access to this information must be approved in advance by the Office of General Counsel and Human Resources, Enterprise Technology Services, or the Chief Privacy Officer.	

<continued>

19. I am responsible for reading, understanding and adhering to UVM's Privacy Policy, Information Security Policy, Information Security Procedures and Computer, Communication, and Network Technology Acceptable Use Policy at all times while utilizing UVM devices or performing work. □

I accept the responsibility of maintaining the integrity, confidentiality, privacy and security of NPPD and to secure UVM-owned and managed devices and services.

Your Signature:____ **Date:**____________________

Manager/Supervisor Signature:_________________________________ **Date:**____________________

<end>