University of Vermont

OFFICE OF COMPLIANCE AND PRIVACY SERVICES
www.uvm.edu/compliance
12 Centennial Woods Way, Room 254, Burlington, VT 05405
P: (802) 656-3086 • E: compliance@uvm.edu

Privacy

This Confidentiality Agreement ("Agreement") is designed to help you understand UVM's policies and our collective responsibilities for safeguarding non-public protected data, or NPPD as defined in UVM's Privacy Policy. By understanding the requirements, you'll be contributing to a secure and trustworthy environment, ensuring that information that needs to be safeguarded, whether it be by university policy or by federal, state, or international regulations, remains protected. This acknowledgment not only helps you maintain the integrity of the information that we have been entrusted with but also fosters a culture of trust and respect. Any questions can be directed to your supervisor or to the Office of Compliance and Privacy Services at privacy@uvm.edu.

Privacy and Confidentiality Agreement

1. I acknowledge that 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

2. I acknowledge that:

    a. my job duties require or may allow me to handle (collect, access, use, disclose, store, and/or destroy) 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" as defined in UVM's Privacy Policy.) This may include personnel/employee 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, location of equipment or dangerous materials, maps or drawings of critical infrastructure, security staffing/scheduling data), and/or

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

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

4. I acknowledge that any collection, access, use, disclosure, storage, or destruction of NPPD outside of the scope of my job responsibilities or for which I have not been authorized is strictly prohibited.

5. 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.

6. I understand that, while I may be asked to enter my password myself for reasons such as technical support, I will never be asked to disclose my password to someone else to enter on my behalf. It is especially important that I:

    a. never provide my username or password in response to an email, text or telephone request.

    b. never respond to a dual authentication push unless I have initiated it. Similarly, never give out my authentication codes to anyone.

c. recognize that phishing or other communications designed to trick me into disclosing my credentials can look very real.

d. verify that the communication is legitimate prior to entering my credentials. e. notify UVM Information Security Office at iso@uvm.edu if I am unable to determine the legitimacy of the communication.

7. I recognize that installing unauthorized software, applications or other programs could compromise the security of the information systems. And if I cannot determine whether the software is authorized, I will reach out to helpline@uvm.edu to ask.

8. I understand that I must keep software up to date and that failure to do is a security risk and does not comply with university policy.

9. I acknowledge that I am prohibited from performing system functions outside the scope of my job responsibilities. Unless it is within my job responsibilities, 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 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 I do not need 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. Surfing or looking at records for non-work related purposes (such as curiosity) are strictly prohibited and may have negative consequences both for me and for the individual(s) whose records I have accessed.

12. 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.

13. I acknowledge that sending or forwarding emails outside of UVM that contain NPPD must be sent using a secure method. UVM provides a secure file transfer service that can be used for this purpose. As such, auto-forwarding email to a personal, a non-uvm.edu, a non-med.uvm.edu email address, unless expressly authorized by Enterprise Technology Services (ETS) is prohibited.

14. I acknowledge that using or requiring others to use non-UVM approved cloud-based storage systems such as Google Drive, iCloud, and DropBox, and non-UVM instances of systems such as SharePoint and OneDrive, for sharing or storing of NPPD is prohibited. If I am unsure whether I am using a UVM instance, I should log out and back in using my uvm.edu or med.uvm.edu credentials.

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

    a. ensuring that meetings or conversations related to confidential or personal matters are not held in public places or in settings that make it possible for others to overhear, and

    b. maintaining control of printed, written, and other hard copies of NPPD and ensuring that they not be left in or on desks, printers, common areas, and other places where unauthorized individuals have access.

16. I acknowledge that accessing or using NPPD while working remotely or when using a non-UVM issued or managed device creates additional risks and that I am obligated to comply with UVM policy and to adhere to regulatory requirements regardless of the location in which I am working or the device that I am using. Specifically:

    a. I will not manually download or save files containing high-risk or regulated NPPD* to my personal or non-UVM issued device. Data owners may, at their discretion, further 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.

All high-risk and restricted use NPPD, along with any low or moderate risk NPPD that the data owner has not explicitly permitted, must be saved to an officially supported UVM service. Accessing UVM's centrally managed services, including servers, remotely may require the use of a VPN. *High-risk and regulated NPPD includes data such as Protected Health Information (PHI/HIPAA), Controlled Unclassified Information (CUI), Non-Public Information (NPI/GLBA), Personal Data (PD/GDPR). It also 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.

b. If using a personal device (i.e., laptop, 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.

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.