UNIVERSITY OF MIAMI
OFFICE of PRIVACY
& DATA SECURITY

Privacy & Security Considerations for Telecommuting & Remote Operations

Introduction

The University of Miami continues to take proactive measures to safeguard the health and safety of students, faculty, staff, and the larger community. As national, state and local guidance around COVID-19 continues to restrict gatherings and strengthen social distancing practices, the University is continually assessing its practices and adapting accordingly. In order to keep the University operational, temporary work-from-home arrangements are underway for those whose work can be performed at home.

As the University community transitions to working remotely, it is imperative to keep privacy and confidentiality in mind. Federal privacy laws and regulations, such as FERPA and HIPAA, still apply during this time. This guide is intended to serve as a resource for the University community at large.

For additional guidance, resources or questions, please contact the Office of Privacy and Data Security at privacy@miami.edu.

Note: All remote working arrangements must be pre-approved by an employee's direct supervisor on the Coral Gables and Marine campuses. For UHealth employees, advanced-approval is required from a manager, department chair, or hospital/ ambulatory CEO, as appropriate.

Human Resources

Managers with HR questions related to COVID-19 should contact their HR Partner or the Employee Accommodations Manager, Mike Gigante.

Telecommuting

Employees who telecommute or work remotely must comply with all University of Miami policies and procedures, including adequately safeguarding and securing any sensitive or confidential information with which they work in accordance with applicable law. Sensitive information includes, but is not limited to, Protected Health Information (PHI), Personally Identifiable Information (PII) of employees, research participants, students and job applicants, and non-public University information including salary details and internal plans.

Below are some reminders for employees working remotely:

- Use University-managed devices when accessing or storing confidential data, including PHI and PII.
- Be mindful when sharing devices with family or friends and remember that University-issued devices should **only** be used by the employee to which they were issued.
- The University of Miami's virtual private network (VPN), Pulse Secure, should only be used by system administrators or for remote access to University on-premise systems/servers. VPN is no longer required for off-campus access to University enterprise systems, including but not limited to: Workday; CaneLink; Microsoft Office 365/Email/Teams; Epic/UChart; Blackboard; Adobe Creative Cloud; cloud storage like Box, OneDrive, and Google Drive; and Zoom. Enterprise systems may be accessed directly by logging in through Single Sign-on.
- Avoid logging in from public places where confidential information may be viewed.
- Many conversations that previously took place in person will now be phone conversations or conference calls. Always make sure all sensitive conversations take place in private or behind closed doors to prevent eavesdropping.
- Only use secure applications for work-related messaging, such as Skype for Business or Microsoft Teams.
- Always secure any physical documents and storage devices, including laptops, that contain confidential University data during non-working hours.
- Lock your doors when you leave! Even if you're just running to the car, it is vital to secure your home and workspace.
- Store electronic documents in University-approved cloud storage solutions (you must use your UM credentials) to minimize the use of paper, which can be easily lost or stolen.

- Always encrypt when possible! Encryption is the best defense to protect against access by unauthorized individuals.
- Monitor participants on teleconference calls to reduce the chance of unauthorized persons on the calls.
- When videoconferencing, always be mindful of others who may not wish to be visible or recorded in the background. Utilize virtual background features (available through Zoom) to prevent having surroundings or others visible.
- Orient computer screens and mobile devices to reduce the chance of “shoulder-surfing.”
- On-campus deliveries should only be scheduled when staff are present and able to receive them.
- Ensure campus mail is not left unattended. Make arrangements to acquire or secure department correspondence.
- Immediately report lost or stolen devices and/or loss of any University information.

Academic Operations

The University provides options for faculty to teach and supports students during emergencies and unplanned disruptions to classes.

Virtual Class & Content Delivery

Faculty and students should reference the Academic Continuity Guide for information on the various remote technologies available to the academic community.

- Platforms that have not been vetted by the University should not be used.
- Personal devices should not be used to record classes. Any recordings should only be stored on University-approved devices or storage solutions.
- Students should be informed that the session will be recorded and provide their written consent to recording prior to the start of a recorded session.
- Students that do not wish to be recorded should be provided alternate means of participation (e.g., submitting questions and comments online).
- Students who request not to be identified on recordings should not be required to use their name or their camera during virtual class.
- Be mindful of others who may not wish to be visible or recorded in the background. Utilize virtual background features (available through Zoom) to prevent having surroundings or others visible.

Monitoring Academic Integrity

Faculty utilizing remote assessment methods may be interested in incorporating technologies that promote students' academic integrity in quizzes, tests, and written work. The University offers various platforms to promote academic integrity, including control of the testing environment.

Many proctoring technologies use machine learning, student behavior patterns, key-logging, application usage, and other technologies to detect academic integrity. Faculty must provide notice to the students before utilizing these technologies.

Online Security

Working remotely presents various cybersecurity challenges that can be different from on-campus work. It is vital that the University community remains vigilant against adversaries seeking to take advantage of the current health crisis.

Phishing

One of the biggest threats to the remote worker is phishing emails. Phishing emails are scam emails that appear to be from a legitimate company and ask you to provide sensitive information. Below are some tips on how to recognize and avoid falling victim to phishing attempts:

- **Poor grammar and syntax**. Poor wording or numerous misspellings are a dead giveaway.
- **Vagueness**. If the subject of the email or any attachments are suspiciously nonspecific and don't reference anything familiar, it is likely a scam.
- **Recognizable name but strange content**. It's easy for criminals to fake the email address of someone you're already in contact with. If the message seems out of character, asks for your personal information or for you to click a strange link, then it's probably a phishing attempt.

Social Engineering

One of the greatest risks to be aware of while working remotely is social engineering attacks. Social engineering is the act of tricking or fooling someone into making a mistake, either electronically or in person. Social engineering broadens the scope from phishing attacks to include phone calls, text messages, social media and fake news. Attacks of these nature are made easier during a time of change and confusion. Some common examples include:

- **Tailgating**: One or more person(s) follows an authorized person through a secured door or other entrance.

- **Shoulder Surfing**: Direct observation techniques, such as looking over someone's shoulder to get information.
- **Impersonation**: A person pretends to be someone they are not in order to gain information.

Strong Passwords

Weak passwords continue to remain the most vulnerable entry-point to any information system and the primary drivers for breaches on a global scale. Choose strong and complex passwords.

- Do not share your passwords - it is a violation of policy!
- Create strong, complex passwords that contain a combination or upper and lowercase letters, numbers and special characters.
- Avoid using personal information, familiar names or number sequences.
- Change passwords frequently to prevent unauthorized users from using automated tools to guess your password. Policy requires passwords to be changed at least every 90 days.
- Multi-Factor Authentication (MFA) creates a layered defense against unauthorized users accessing your information.
- If you suspect your password is compromised, change it immediately and contact UMIT at 305-284-6565 or UHealth IT at 305-243-5999.

Patient Care & HIPAA Guidance

HIPAA Privacy and Security Rules still apply during a public health emergency such as a disease outbreak. Employees who provide patient or student health care must continue to abide by all applicable University Privacy policies, laws and regulations.

Please remember that the "minimum necessary" standard is one of the cornerstones of HIPAA and always applies when sharing patient information. Only share the minimum information necessary to accomplish the goal at hand!

For further guidance on HIPAA and patient privacy, contact the Office of Privacy and Data Security at 305-243-5000.