



University Community (faculty and staff)

SUBJECT (R*)	EFFECTIVE DATE (R*)	GUIDELINE # (O*)
Information Technology Guideline for Remote Access & Work from Home	3/10/2020	IT-7.6

APPLICATION (R*)

The guidelines specified in this document apply to all University employees (faculty, staff, and persons-of-interest) that require access to network resources and/or data from outside Florida International University premises. This includes but is not limited to employees working remotely or from home.

PURPOSE (R*)

The purpose of this document is to formalize the FIU approach to remote access (including work from home) in ways that promote effective access to online resources for FIU employees while also ensuring necessary IT security. This guideline describes the supported approaches to connectivity, data storage, collaboration, and more. Also, included is a remote access self-assessment checklist to help you identify the IT requirements based on the FIU resource you need to access (see appendix 1). Appendix 2 lists the IT hardware and software supported requirements for remote access.

BACKGROUND (O*)

- CONTENTS (O*)**
1. Connectivity (connect to FIU resources remotely)
 2. Data Storage (files and documents)
 3. Collaboration Tools
 4. Video Conferencing
 5. Telephony (FIU Office phone number)
 6. Support
 7. Appendix 1 – Remote Access Self-Assessment Checklist
 8. Appendix 2 – Remote Access Matrix

1. Connectivity (connect to FIU resources remotely):

There are several supported ways to connect and access FIU resources and data from off campus locations. The method used to connect depends which FIU resources and data you are accessing:

1. Publicly Accessible Sites/Resources via a web browser can be accessed from a personally owned device (POD) connected to the internet through a web browser. This includes but is not limited to [Canvas](#), [AskIT](#), and [MyFIU](#).
2. Internal Resources can be accessed through one of two ways. Access to these internal resources may apply to certain workgroups. If you have any questions, please contact your local IT administrator or the Division of IT.
 - a. A **laptop computer joined to Active Directory** provided to the user by his/her IT unit administrator which meets the minimum hardware requirements stated above.
 - i. Virtual Private Network (VPN) is required to access any internal or non-publicly accessible FIU Resources and sites from off campus locations. [Click here](#) for information on how to use the VPN.
 - ii. Two-Factor Authentication (2FA) is required for VPN access.
 - b. Utilize the **Enterprise Virtual Desktop Infrastructure (VDI)** for remote access through any web browser on any device such as personally owned laptops, computers, and tablets. [Click here](#) for information on how to use VDI.
 - i. There is a monthly recurring cost of \$20.00 per month per user for VDI.
 - ii. Two-Factor Authentication (2FA) is required to access a virtual desktop. For information on how to enroll in two-factor authentication [click here](#).

2. Data Storage (files and documents):

All FIU related files and documents must be stored in OneDrive, an Active Directory file share, or SharePoint Online. This not only provides data security for those files and documents but also allows you to access those files from FIU and when working remotely. [Click here](#) for information on how to use OneDrive.

3. Collaboration Tools:

Office 365 (mail.fiu.edu) offers several collaboration tools to help you collaborate on documents, spreadsheets, and presentations with other people. Use the Office365 collaboration tools such as Teams and OneDrive to collaborate with others.

- a. [Microsoft Teams](#) is a unified communication and collaboration platform that combines persistent workplace chat, video meetings, file storage (including collaboration on files), and application integration. Teams is a great way to collaborate with team members, committee members, and employees in other departments. For more information on how to use Teams for collaboration [click here](#).
- b. OneDrive is a place to store files and share files. You can collaborate on files shared in OneDrive with those you shared the files with. [Click here](#) for information on how to share files with OneDrive.

4. Video/Audio Conferencing:

Host and participate in meetings while working remotely with Zoom or Microsoft Teams, the supported video conferencing tools.

- a. [Zoom](#) is a cloud platform for video and audio conferencing. It can be used on mobile devices, desktops, and laptops. [Click here](#) to get started with Zoom to host or join a video conference.
- b. [Microsoft Teams](#) can also be used for video and audio conferences. It can be used on mobile devices, desktops, and laptops. [Click here](#) to learn how to make video and audio calls with Teams.
- c. [Audio Conferencing](#) offers on-demand conferencing, allowing users to initiate a conference call 24 hours a day 7 days a week - without the need to make a reservation. The conference call will have no time limits, and each call can handle up to 500 participants. [Click here](#) for more information about audio conferencing.

5. Telephony (FIU Office phone number):

When working remotely there are a couple of ways to stay up to date with calls being placed to your FIU office phone number.

- a. FIU office phone numbers can be forwarded to a personal mobile phone or landline. [Click here](#) for instructions on how to forward your office phone number.
- b. If your phone number has voicemail capabilities, you can listen to voice messages remotely or have your voicemail recordings delivered to your FIU email. [Click here](#) for more information on available voicemail features.
 - i. Ensure that the you have access to your voicemail to hear voice messages.
 - ii. Enable unified messaging to have voicemail recordings delivered in your email. To request this feature on your office phone number [click here](#).
 - iii. Ensure that you have access to modify your [voicemail greetings](#).

6. Support:

All the services listed above are supported by the Division of IT Support Center. For assistance with any of the items call the Division IT Call Center at 305-348-2284 or visit the [AskIT Knowledge Base](#).

DEFINITIONS (R*)

Active Directory (AD) Joined Laptop: Laptops which have been configured to join to the FIU Active Directory Domain. These laptops also have the required security tools, patches and applications along with a standard configuration.

Enterprise Virtual Desktop: is a computer that you access and operate over the internet.

Virtual Private Network (VPN): FIU's Virtual Private Network (VPN) provides safe and private access to the University's network while off campus. This is useful if you are not on campus and need access to University resources.

Personally Owned Device (POD): A computer or mobile device not procured or issued to an employee through FIU. Personally owned includes devices for which a user receives a university subsidy or stipend as well as those fully owned by the employee.

Two-Factor Authentication (2FA): 2FA increases the safety of your account by requiring an additional layer of security that helps minimize the risk of comprised credentials caused by phishing, social engineering, and password attacks. Increased security measures on your account by requiring two steps to log in to your FIU services: something you know (your password) and something you have (a physical device, like your smartphone).

Sensitive Data: Information that in isolation may not present any specific risk to the confidentiality, integrity or availability of university operations, resources, or constituents but if combined with other data could represent inappropriate risk.

Confidential Data: Information that if lost, disclosed, or inappropriately modified could cause significant impact to the confidentiality, integrity, availability of university operations, resources or constituent.

Web Based: These are resources which are accessible via a web browser through an internet connection from anywhere.

Internal Resources: These are resources which are only available when on campus connected to the FIU network or via VPN. These are not publicly accessible resources. These internal resources are specific to certain workgroups but does not apply to all.

Collaboration Tools: Tools that help a group of people collaborate on documents, projects, tasks, etc.

OneDrive: Personal storage to allow safely storing documents in FIU's O365 cloud environment. This is available to all FIU personnel. It is accessible via web browser (Visit mail.fiu.edu) and via the OneDrive client app. OneDrive offers users a simple way to store, sync and share various types of files, with other people and devices on the internet.

Microsoft Teams: Available to all FIU personnel via the University's O365 environment and is accessible via web browser (Visit mail.fiu.edu) and via the Teams client app. Teams support IM conversation, sharing of documents with colleagues and group collaboration tools including online meetings and video chats for up to 80 participants.

Zoom: A reliable cloud platform for video and audio conferencing, collaboration, chat, and webinars across mobile devices, desktops, telephones, and room systems. This tool also allows faculty, staff, and students to host video conferences from your own devices and offers multiple integration options including [Outlook](#), [Google](#), and [Canvas LMS](#).

Audio Conferencing: offers on-demand conferencing, allowing users to initiate a conference call 24 hours a day 7 days a week - without the need to make a reservation. The conference call will have no time limits, and each call can handle up to 500 participants.

Call Forwarding: A telephony feature to redirect a telephone call to another destination, such as your mobile phone.

Unified Messaging: With this feature, FIU's voicemail system will integrate seamlessly to your email inbox, allowing you to access your voicemail within your email inbox.

REFERENCES (O*)

Hardware requirements for laptops: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010712

FIU PantherTech: Your On-Campus Tech Store: https://fiu.service-now.com/sp?id=kb_article_view&sysparm_article=KB0010539

Two Factor Authentication (2FA): https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010358

Getting started with Enterprise Virtual Desktop: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0011391

Getting Started with VPN: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0011249

Getting Started with OneDrive: https://fiu.service-now.com/sp?id=kb_article_view&sysparm_article=KB0010638

Voicemail: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010534

Voicemail Greeting: https://fiu.service-now.com/sp?id=kb_article&sys_id=978ae0bedbf37fc4ff70785e0f961924

Call Forwarding Instructions: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010537

Request Unified Messaging: [https://fiu.service-](https://fiu.service-now.com/sp?id=sc_cat_item&sys_id=4219e227db79fa0027763c00ad9619d6&sysparm_category=24e3bd93db99aa00217e70e21f96193d)

[now.com/sp?id=sc_cat_item&sys_id=4219e227db79fa0027763c00ad9619d6&sysparm_category=24e3bd93db99aa00217e70e21f96193d](https://fiu.service-now.com/sp?id=sc_cat_item&sys_id=4219e227db79fa0027763c00ad9619d6&sysparm_category=24e3bd93db99aa00217e70e21f96193d)

Audio Conference Calling: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010533

Microsoft Teams: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010563

How to Collaborate in Teams: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0011385

How to Share Files with OneDrive: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010638

Getting Started with Zoom: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0011097

HISTORY (R*)

3/10/2022: Guideline Effective Date

3/16/2020: Version 2 added audio conferencing and Remote Access checklist

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)

Division of Information Technology

RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)

Division of Information Technology
11200 SW 8 ST, PC531, Miami, FL 33199
Telephone Number: 305-348-2738

*R = Required *O = Optional

Remote Access Self-Assessment Checklist

Please review the Remote Access checklist below to assess if you have the technology requirements needed to work remotely. Depending on the FIU resource you need access to, Two-Factor Authentication (2FA) will be required. Enroll in 2FA today, if you have not done so already.

Check all the FIU resources you primarily need to access to determine what you need to access those resources.

Data Classification	FIU Resource	IT Requirements
Level 1 - Public	<ul style="list-style-type: none"> <input type="checkbox"/> Public websites <input type="checkbox"/> MyFIU <input type="checkbox"/> Canvas <input type="checkbox"/> FIUmail <input type="checkbox"/> OneDrive <input type="checkbox"/> Zoom <input type="checkbox"/> Teams 	Personal Device or FIU managed laptop joined to AD or Virtual Desktop (VDI)
Level 2 - Internal	<ul style="list-style-type: none"> <input type="checkbox"/> File Shares <input type="checkbox"/> ImageNow Client <input type="checkbox"/> Topaz Client <input type="checkbox"/> Graphic-Intensive Systems (I.e photoshop, autocad) 	FIU managed laptop joined to AD with VPN or Virtual Desktop (VDI)
Level 3 - Sensitive & Confidential	<ul style="list-style-type: none"> <input type="checkbox"/> Student Data <input type="checkbox"/> Financial Data <input type="checkbox"/> Research Data <input type="checkbox"/> Health Data <input type="checkbox"/> Personal Identifiable Data <input type="checkbox"/> Other Sensitive or Confidential Data <input type="checkbox"/> Administer Servers <input type="checkbox"/> Administer Applications <input type="checkbox"/> Administer Databases <input type="checkbox"/> Call Centers (Support Center, OneStop, Online, etc) 	FIU managed laptop joined to AD with VPN

APPENDIX 2

1. Minimum Hardware Requirements for Workstations:

These are the Minimum Supported Hardware Requirements for workstations being joined to FIU's active directory (AD).

Tech Specs	Dell/HP/Lenovo*	Apple
Processor	Intel® Core™ i5	Intel® Core™ i5
Chip	Dell: TPM 2.0	N/A
Memory	8 GB	8 GB
Storage	Minimum 256GB SSD	Minimum 256GB SSD
Graphics	Intel® HD Graphic	Intel® HD Graphic
Operating System	Windows 10 Professional	macOS Mojave (10.14)

* All systems must be business use models such as Dell Latitude. Consumer models such as Dell Inspiron are not supported.

To purchase a workstation which meets these requirements visit the [PantherTech Store](#)

2. Supported Remote Access Matrix (supported ways to access FIU resources remotely):

Below is a matrix to assist you determine which of the remote access option best fits your needs based on FIU resources being accessed and worked on remotely.

	FIU Managed Laptop (AD Joined)	Enterprise Virtual Desktop (VDI)* ∇Δ	Personally Owned Device*^
Web Based Resources (i.e. PantherSoft, Canvas, AskIT, CBord, Raiser Edge, Nupark, etc)	√	√	∩ Institutional information must be saved in OneDrive, otherwise does not meet requirements
Collaboration and Productivity Tools (i.e. Web Mail, O365, OneDrive, Teams, Zoom, etc.)	√	√	∩ Institutional information must be saved in OneDrive, otherwise does not meet requirements
Access to Sensitive and Confidential Data (i.e. electronics protected health information, financial, student records, employee records, legal documents, research data, Personal Identifiable Information (PII))	√ VPN is Required	√	∅
Internal Resources (Only available while connected to the FIU network or via VPN)	√ VPN is Required	√	∅
Graphics-Intensive Systems (i.e. Photoshop, AutoCAD, etc.)	√	∩ May require single user configuration at additional cost	∅
Call Centers (I.e. Support Center, OneStop, Online Call Center)	√ VPN is Required	∅	∅

√ Fully meet requirements Fully Supported by DoIT	∩ Partially meet requirements Partially Supported by DoIT	∅ Does not meet requirements Not Supported	∇ Accessed from Personally Owned Device * FIU data must be saved on OneDrive Δ Monthly recurring cost per user ^ Personally Owned Devices should maintain up to date patches and device appropriate security measures
---	---	--	--

