FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY GUIDELINE

University Community (faculty and staff)

SUBJECT (R*)	EFFECTIVE DATE (R*)	GUIDELINE # (O*)
Off-Site FIU IT Equipment Security Guideline	3/23/2020	IT-2.1.6

APPLICATION (R*)

The guidelines specified in this document apply to any University employees (faculty, staff, and persons-of-interest) that need to take FIU owned IT equipment off-site in order to perform their work duties remotely. Any workstations being taken off-site will only be used to access network resources and/or data from outside Florida International University premises.

PURPOSE (R*)

The purpose of this document is to formalize the FIU process in which FIU IT equipment can be taken off-site for remote-work use. This guideline provides a list of security controls required to maintain the confidentiality, integrity, and availability of the FIU resources and data being accessed. In addition, this guideline lists the supported approaches to remote-access connectivity, data storage, backup, and much more.

BACKGROUND (O*)

CONTENTS (O*)

1. Off-Site IT Equipment

Any Workstation or IT equipment should not be taken off-site without prior management authorization. We do not recommend taking any FIU desktop computers off-site, but in the event a user needs to in order to facilitate remote access to FIU resources and data, the Off-Site IT Equipment Request form must be submitted and approved prior to taking the desktop from FIU premises.

a. Workstations (Desktops and Laptops)
   i. FIU workstations must be joined to the FIU active directory domain (AD).
   ii. Appropriate security measures should be applied to workstations being removed from university premises, taking into account the different risks of working outside the University premises.

b. University IT equipment taken off-site must be used only for University business.

c. Fill out the Off-Site IT Equipment Request form here.
   i. As per FIU Procedure 1130.010a, Use of University Property Off-Campus, if equipment is over $5,000, the Off-Campus Property control form must be filled out. See Appendix 3.
   ii. The manager or supervisor must approve the off-site request.

d. The user must log in (authenticate) to the workstation from campus at least once prior to the workstation being taken off-site.
   i. If the user doesn't log in at least once while on the FIU network, they will not be able to log in to the workstation off-site.
   ii. This can be done on the wired or FIU Secure Wi-Fi wireless network.

e. Review the Desktop Off-Site Checklist (appendix 4) to verify that you are taking all the cables and peripherals for the desktop.

f. The IT equipment must be returned to its campus location as soon as the off-site work is completed or within one day of request made by the Division of IT or the employee's supervisor.

2. Responsibility of IT Equipment Taken Off-Site

While the IT equipment is off-site, the employee is responsible for the security of the equipment, and its appropriate use and maintenance.

a. Workstations and IT Equipment removed from University premises is particularly vulnerable to loss or theft. The IT equipment must be protected when off-site, at home, or while in transit from one location to another.

b. If loss or theft occurs, file a police report and contact the IT Security Office at security@fiu.edu or 305-348-1366.

3. 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 on which FIU resources and data you are accessing. If you have any questions, contact your local IT administrator or the Division of IT.

a. Wi-Fi Adapter will be required if the FIU desktop will be joined to Wi-Fi network. Most desktop computers do not have one built in. Contact PantherTech to purchase a USB Wi-Fi adapter for the desktop.

b. Publicly Accessible Sites/Resources via a web browser can be accessed from a through a web browser. This includes but is not limited to Canvas, AskIT, and MyFIU.

c. Internal Resources must be accessed through the virtual private network (VPN). Click here for information on how to use the VPN.
   i. Two-Factor Authentication (2FA) is required for VPN access. For information on 2FA click here.

4. Data Storage (files and documents)

All FIU related files and documents must be stored on OneDrive, an Active Directory file share, or through 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. To learn more about how to use OneDrive, Click here.

5. Remote Access Cybersecurity Tips:

a. Home Networks
   i. Review the Secure your Home Network document.
   ii. Reset default Wi-Fi Router passwords.
   iii. Do not share work computers with others in the home.

b. Be aware of phishing and social engineering attacks that you may receive. To learn more about phishing and its many forms, visit https://security.fiu.edu/phishing.

c. Backup your data.
    i. Use Crashplan to backup your data. Click here for more information on crashplan.

d. Do not plug unknown USB drives into your computer.

e. Updates to FIU managed AD joined devices are installed after business hours. In order to make sure that all FIU managed AD joined devices are updated and patched, lock the screen or log off after you are finished working, (do not shut it down).

f. Enable Two-Factor Authentication (2FA) whenever possible and where supported. To learn more about (2FA) click here.

g. Complete the Cybersecurity Awareness Training.

h. In the event of an incident, contact the FIU IT Security Office at security@fiu.edu or 305-348-1366.

6. Support:

All the services listed above are supported by the Division of IT Support Center. For assistance with any of these items contact the Division of IT online or by calling 305-348-2284 during their normal working hours.

DEFINITIONS (R*)

Off-Site: A geographical location other than on FIU campuses.

IT Equipment: Desktops, laptops, printers, scanners, and other IT assets.

Active Directory (AD) Joined Workstations: Desktops or 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.

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.

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.

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.

REFERENCES (O*)

Off-Site IT Equipment Request

Use of University Property Off-Campus, FIU Procedure 1130.010a
FIU PantherTech: Your On-Campus Tech Store: https://fiu.service-now.com/sp?id=kb_article_view&sysparm_article=KB0010539
Phishing: https://security.fiu.edu/phishing
FIU IT Security Web Site: https://security.fiu.edu
FIU Division of IT Remote Work: https://it.fiu.edu/remote-work
Two Factor Authentication (2FA): https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010358
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
How to Share Files with OneDrive: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010638
Cybersecurity Awareness Training: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010450
Crashplan: https://fiu.service-now.com/sp?id=kb_article&sysparm_article=KB0010180

HISTORY (R*)

3/23/2020: Guideline Effective Date

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**

APPENDIX 1

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	❑ Public websites ❑ MyFIU ❑ Canvas ❑ FIUmail ❑ OneDrive ❑ Zoom ❑ Teams	Personal Device or FIU managed workstation joined to AD or Virtual Desktop (VDI)
Level 2 - Internal	❑ File Shares ❑ ImageNow Client ❑ Topaz Client ❑ Graphic-Intensive Systems (i.e photoshop, autocad)	FIU managed workstation joined to AD with VPN or Virtual Desktop (VDI)
Level 3 - Sensitive & Confidential	❑ Student Data ❑ Financial Data ❑ Research Data ❑ Health Data ❑ Personal Identifiable Data ❑ Other Sensitive or Confidential Data ❑ Administer Servers ❑ Administer Applications ❑ Administer Databases ❑ Call Centers (Support Center, OneStop, Online, etc)	FIU managed workstation 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 Device (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

APPENDIX 3

FLORIDA INTERNATIONAL UNIVERSITY / PROPERTY CONTROL

I. AUTHORITY FOR UNIVERSITY PROPERTY TO BE USED OFF–CAMPUS

Permission is requested to use the following listed equipment off-campus valued at $5,000.00 or more.

FIU Tag No.	Description	Serial No.	Value	Activity Nbr/Project ID
1. 4980- _____	_____	_____	_____	_____
2. 4980- _____	_____	_____	_____	_____
3. 4980- _____	_____	_____	_____	_____
4. 4980- _____	_____	_____	_____	_____
5. 4980- _____	_____	_____	_____	_____

(If necessary, attach an additional sheet)

Purpose: _____

Location: _____ Telephone: _____
Street address

_____ Period of use: from _____ to 06/30/2020
City State Zip Code

1. I certify that the equipment listed above will be used for an official university purpose and will be returned to the University as soon as the project is completed.
2. I hereby acknowledge the receipt of the above listed property and am aware of the responsibility for its care and return. **See below for notification of returned property.**

_____ | _____ | _____@fiu.edu
Date | Signature of Requestor | E-mail address

_____ | _____ | _____ | _____
Department Name | Name (print) | Panther ID | Title

Check one: ☐ USPS ☐ Faculty ☐ A&P ☐ Other (explain) _____

Equipment listed herein is the property of the Florida International University under the provisions of Fla. BOG Reg. 9.002. Damage or loss of this property must be immediately reported to the Accountable Officer who is the custodian for this property. Personal liability may be assessed if gross negligence or lack of due care is proven in the use of this equipment.

II. AUTHORIZATION

Permission is hereby granted to the person listed above for the OFF- Campus use of the equipment herein requested for the time period indicated above

_____ | _____ | _____@fiu.edu
Date | Signature of Expense Manager/Project Manager | E-mail address

_____ | _____ | _____ | _____
Department Name | Name (print) | Panther ID | Title

III. NOTIFICATION OF RETURNED PROPERTY

I hereby certify that all the property listed has been returned in satisfactory condition to the following location

_____ | _____ | _____ | _____
Date | Building location | Received by | Panther ID | Phone

Return completed form to:
PROPERTY CONTROL
MODESTO MAIDIQUE CAMPUS, CSC–1140
Office: (305) 348–2167 Fax: (305) 348-1936
Email: property@fiu.edu

APPENDIX 4

Desktop Off-Site Checklist

If you are taking a desktop computer off-site verify that you have completed the following:

- ❑ Filled out the Off-Site IT Equipment Form
- ❑ Joined to AD and logged in at least once to this workstation.

In order for your desktop computer to work off-site make sure you take the following with you.

- ❑ Monitor
- ❑ Monitor Power Cable
- ❑ Keyboard
- ❑ Mouse
- ❑ Desktop
- ❑ Desktop Power Cable
- ❑ WiFi Adapter (not all have one, it may need to be purchased. Call PantherTech to purchase one.