


UNIVERSITY OF MIAMI 	FRM-SEC-NSD-505-02	
	Information Technology	
	Effective Date: 04/15/2019	Page 1 of 6
Document Title: Non-Standard Device Questionnaire		

Date:

Incident #:

First Name:

Email Address:

Last Name:

Telephone #:

Department:

Job Title:

Requested Device Type (Select One):

Computing Device (e.g. Laptop / Tablet)

*Data Storage Device (e.g. External Hard Drive / USB Flash Drive)


Manufacturer:

Model or Part Number:

Please provide a detailed description of the use or purpose of the device:

* UMIT offers cloud based file sharing and storage solutions to all faculty, staff, and students through Box: box.miami.edu, Microsoft OneDrive: drive.miami.edu, and Google Drive: google.miami.edu. A Business Associate Agreement (BAA) exists with these vendors. Pre-approved Data Storage Devices (DSDs) are available in Workday (UMarketplace) catalog.

**<https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>

	FRM-SEC-NSD-505-02	
	Information Technology	
	Effective Date:	Page 2 of 6
Document Title: Non-Standard Device Questionnaire		

Regulatory Compliance:

What kind of data will be stored/handled on requested device? (Check all that apply)

- Academic Data Financial Data Clinical Data Research Data
- Administrative Intellectual Property Confidential Business Information
- Other:


**Will you be travelling abroad with requested device?
 YES NO

If you answered “YES” above, will you be travelling to one or more of the following sanctioned countries? (North Korea, Iran, Sudan, Syria, Venezuela, Russia or any other countries detailed in the Sanctions Programs and Country Information page maintained by the US Department of the Treasury - <https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>)
 YES NO N/A (Answered No Above)

If answered “YES” above, Please attach written approval from Export Compliance at exportcontrol@miami.edu to this questionnaire! (<https://www.ora.miami.edu/compliance/export-control-compliance/travel-and-export-compliance/index.html>)

* UMIT offers cloud based file sharing and storage solutions to all faculty, staff, and students through Box: box.miami.edu, Microsoft OneDrive: drive.miami.edu, and Google Drive: google.miami.edu. A Business Associate Agreement (BAA) exists with these vendors. Pre-approved Data Storages Devices (DSDs) are available in Workday (UMarketplace) catalog.

**<https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>

UNIVERSITY OF MIAMI 	FRM-SEC-NSD-505-01	
	Information Technology	
	Effective Date:	Page 3 of 6
Document Title: Non-Standard Device Questionnaire		

Will you be storing/handling any data on the requested device that falls under any of the following mandates? (Select All That Apply)

Personally Identifiable Information (PII): Will you be storing any piece of information contained in the Protected Data which can be potentially used to uniquely identify, contact, or locate a single person. Examples of PII include First and Last Name or First Initial and Last Name plus Protected Health Information (PHI), Credit Card Numbers, Social Security Numbers (SSNs), etc.

HIPAA - (The Health Insurance Portability and Accountability Act of 1996 with the purpose of ensuring the privacy of a patient’s medical records.)

FERPA – (The Family Educational Right and Privacy Act of 1974 with the purpose of protecting the privacy of student education records.)

GLBA – (The Gramm-Leach Bliley Act, also known as the Financial Services Modernization Act of 1999, contains privacy provisions requiring the protection of a consumer’s financial information.)

PCI-DSS – (Payment and Credit Card Industry Data Security Standards is guidance developed by the major credit card companies to help organizations that process card payments; prevent credit card fraud, hacking, and various other security issues. A company processing card payments must be PCI compliant or risk losing the ability to process credit card payments.)


FISMA – (The Federal Information Security Management Act of 2002 recognizes the importance of information security to the economic and national security interests of the United States and as a result sets forth information security requirements that federal agencies and any other parties collaborating with such agencies must follow in an effort to effectively safeguard Information Technology systems and the data they contain.)

FDA Part 11 – (The Food and Drug Administration guidelines on electronic records and electronic signatures.

Data Use or Data Sharing Agreement – Contractual agreements between Universities, Industries, and Government entities. *i.e., Data collected per commercial agreement, data collected per government agreement, Controlled Unclassified Information.*

* UMIT offers cloud based file sharing and storage solutions to all faculty, staff, and students through Box: box.miami.edu, Microsoft OneDrive: drive.miami.edu, and Google Drive: google.miami.edu. A Business Associate Agreement (BAA) exists with these vendors. Pre-approved Data Storage Devices (DSDs) are available in Workday (UMarketplace) catalog.

**<https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>

	FRM-SEC-NSD-505-02	
	Information Technology	
	Effective Date:	Page 4 of 6
Document Title: Non-Standard Device Questionnaire		

AGREEMENT

Requested device shall meet UMIT minimum standards as determined by UMIT.

If the requested device falls under regulatory compliance mandates, the device must be UMIT centrally-managed for security requirements (anti-virus, mobile device management, encryption, and mandated security controls) and these will not be disabled.

If the device does not fall under regulatory compliance or mandates, you will be responsible for the security, maintenance, data backup, recovery, and technical support.

You agree to perform up-to-date software patch management along with manufacturer device updates.

UMIT must be notified immediately if the device is lost or stolen by contacting (305) 284-6565, (305) 243-5999, or via email at CISO@miami.edu.

It is your responsibility to make the proper arrangements with UMIT to implement security controls.

You understand that by UMIT opening, installing, or otherwise altering a computing device after receipt from a manufacturer or vendor, it may make the product ineligible for return.

You understand that if the requested device does not fall under Dell's "Keep Your Hard Drive" program, you agree that the computing device (either storage sub system or the entire device) cannot be sent to the vendor for repair or replacement.

If storing/handling regulatory, protected, sensitive, or contractual data; you will adhere to the mandates of applicable legislative University policies and contractual obligations.


UMIT reserves the right to audit this request for compliance with the parameters and constraints provided to use as the basis for this request and verify that all the appropriate security measures such as, but not limited to, anti-virus and encryption are installed and working properly.

This form is governed by applicable UMIT Policies and Procedures. For additional information, please visit the Policies and Procedures section of the UMIT website. (<https://it.miami.edu/about-umit/policies-and-procedures/index.html>)

I agree and will adhere to the requirements above:

* UMIT offers cloud based file sharing and storage solutions to all faculty, staff, and students through Box: box.miami.edu, Microsoft OneDrive: drive.miami.edu, and Google Drive: google.miami.edu. A Business Associate Agreement (BAA) exists with these vendors. Pre-approved Data Storage Devices (DSDs) are available in Workday (UMarketplace) catalog.

**<https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>

	FRM-SEC-NSD-505-01	
	Information Technology	
	Effective Date:	Page 5 of 6
Document Title: Non-Standard Device Questionnaire		

Regulatory Compliance Requirements:

Health Insurance Portability and Accountability Act (HIPAA) & Protected Health Information (PII):

Federal Health Insurance Portability and Accountability Act regulations seek to protect the privacy and security of Protected Health Information (PHI). HIPAA establishes requirements for covered entities, such as health care providers, regarding the release of PHI to non-employee business associates. PHI is individually identifiable health information that relates to the pasts, present, or future physical or mental health/condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual.

Gramm Leach Bliley Act (GLBA):

Pursuant to Federal laws, The University of Miami has a duty to protect all non-public, personally identifiable financial information. Examples of non-public personal information include Social Security Number, financial account numbers, credit card numbers, date of birth, name, address, phone number when collected with financial data, details of financial transactions.

Family Educational Rights and Privacy Act (FERPA):

Family Educational Rights and Privacy Act is a federal law that protects the privacy and security of student education records. Education records are defined as records, files, documents, and other materials that contain any information directly related to a student, and are maintained by education agency or institution, or by a person acting on behalf of an agency or institution. These include, but are not limited to: transcripts, grades, exam papers, test scores, evaluations, financial aid records and loan collection records. The law requires that student education records be shared only between the student and those who have a legitimate education-related interest.

Payment Card Industry Data Security Standard (PCI-DSS):

The PCI-DSS requires the protection of payment/credit card data and related account information. Examples include information provided on an application for a credit card, payment history, account balance information, cardholder data, and sensitive authentication data.

Intellectual Property:


Intellectual Property refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. Intellectual Property is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the Intellectual Property system aims to foster an environment in which creativity and innovation can flourish.

Academic Data:

Academic Data refers to Academic institutional data surrounding, but not limited to, classroom logistics and infrastructure, course/program curriculum, teaching materials, and any other materials encompassing educational/academic resources. Data protected by FERPA is also considered to be Academic Data.

* UMIT offers cloud based file sharing and storage solutions to all faculty, staff, and students through Box: box.miami.edu, Microsoft OneDrive: drive.miami.edu, and Google Drive: google.miami.edu. A Business Associate Agreement (BAA) exists with these vendors. Pre-approved Data Storage Devices (DSDs) are available in Workday (UMarketplace) catalog.

**<https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>

	FRM-SEC-NSD-505-01	
	Information Technology	
	Effective Date:	Page 6 of 6
Document Title: Non-Standard Device Questionnaire		

Research Data:

Research data is collected, observed, or created, for purposes of analysis to produce original research results. Results are recorded factual material commonly retained by and accepted in the internal and/or external scientific communities as necessary to validate research findings. Research data can be protected by, but not limited to, HIPAA, FERPA, and Intellectual Property.

The Federal Information Security Management Act (FISMA):

The Federal Information Security Management Act of 2002 is part of the Electronic Government Act of the United States that defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats. FISMA assigns responsibilities to various agencies to ensure the security of government data.

Code of Federal Regulations Title 21 Part 11 (CFR 21 Part 11):

The Code of Federal Regulations Title 21 Part 11 is an established regulation by the Food and Drug Administration regulating electronic records and electronic signatures. It defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records.

General Data Protection Regulation:

A European legal framework that sets guidelines for the collection and processing of personal information of individuals. GDPR sets out principles for data management and the rights of the individual.

* UMIT offers cloud based file sharing and storage solutions to all faculty, staff, and students through Box: box.miami.edu, Microsoft OneDrive: drive.miami.edu, and Google Drive: google.miami.edu. A Business Associate Agreement (BAA) exists with these vendors. Pre-approved Data Storage Devices (DSDs) are available in Workday (UMarketplace) catalog.

**<https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>