Non-supported Device (NSD) Questionnaire

First Name: Email Address:

Last Name: Telephone #: Date:

Department/Job Title:

Do you have an Incident or Service Now ticket number for this request? If Yes, Incident #:

Device type ◉ Computing Device (e.g. laptop, tablet) ○ *Data Storage Device (e.g. external hard drive, USB flash drives)

* The University of Miami offers FREE cloud based file sharing and storage solutions to all faculty, staff, and students through Box: box.miami.edu (25GB), Microsoft OneDrive: drive.miami.edu (1 TB), and Google Drive: google.miami.edu (30 GB). A Business Associate Agreement (BIA) exist with these vendors and thus the data is encrypted (at-rest and in-transit). Also, pre-approved Data Storages Devices (DSDs) are available on the UMeNET (Ariba) catalog.

Make and Model

How would this data be classified? (Check all that apply)

- ☐ Production Data
- ☐ Developmental Data
- ☐ Clinical
- ☐ Administrative
- ☐ Research
- ☐ Other

If other, please specify:

Will you be traveling abroad with the device?

◉ Yes ○ No

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

Regulatory Compliance: Will you be storing any data on the device that falls under any of the following mandates? See Page 3 for extended definitions

◉ No	○ Yes	HIPAA (The Health Insurance Portability and Accountability Act of 1996 with the purpose of ensuring the privacy of a patient's medical records.)
◉ No	○ Yes	FERPA (The Family Educational Right and Privacy Act of 1974 with the purpose of protecting the privacy of student education records.)
◉ No	○ Yes	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.)
◉ No	○ Yes	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.)
◉ No	○ Yes	Red Flag (A mandate developed by the Federal Trade Commission (FTC) requiring institutions to develop identity theft prevention programs.)
◉ No	○ Yes	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 IT systems and the data they contain.)
◉ No	○ Yes	FDA Part 11 (Food and Drug administration (FDA) guidelines on electronic records and electronic signatures.)
◉ No	○ Yes	Will you be storing Personally Identifiable Information(PII) on the device? Any piece of information contained in Protected Data which can potentially be used to uniquely identify, contact, or locate a single person. Examples of PII include Protected Health Information (PHI), Credit Card Numbers, Social Security Numbers (SSNs), etc.

Data Classification:

◉ No	○ Yes	Will you be storing Confidential Business Information?
◉ No	○ Yes	Will you be storing any Intellectual Property (IP)?

Do you agree with the following conditions?

Technical Support: At the present, UMIT does not support this device. Therefore, we are approving this purchase with the understanding that you shall secure maintenance, data backup, recovery and technical support from sources outside of UMIT. Although UMIT shall not be providing technical support, please notify us if the device is lost or stolen by calling (305) 243-5999 or (305) 284-6565. You further agree to regularly patch the device as directed by the manufacturer.

Compliance: UMIT reserves the right to audit this device and verify that all the appropriate security measures such as anti-virus and encryption are installed and working properly.

Export Compliance: To avoid any export compliance issues, you agree to contact the Office of Research Compliance for an Export Control review and determination prior to traveling abroad.

Manufacturer/Vendor Return Policies:
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. The Manufacturer or Vendor shall be contacted and an attempt shall be made to secure a return if necessary, but the Manufacturer or Vendor's approval of the return is NOT guaranteed.

Standard Work Procedure (SWP): This form is governed by SWP-UMIT-APFNSD-201-01 - Approval Process for Non-Supported Devices. For additional information, please visit the Policies & Procedures section of the UMIT website.

Encryption (Applicable to Computing Devices only): You understand that your Computing Device shall be encrypted using UM's centrally-managed McAfee or third-party MobileIron application, as applicable, and that you shall not disable this feature. It is your responsibility to make the proper arrangements with UMIT to get this installed. Initials_____.

UMIT reserves the right to audit this request for compliance with the parameters and constraints provided to us as the basis for this request and the conditions stipulated in this document.

If you agree with the conditions above, please sign: _____ _____ _____

Print Name **Signature** **Date (mm-dd-yy)**

Regulatory Compliance Definitions:

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

Federal Health Insurance Portability and Accountability Act (HIPAA) 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 nonemployee business associates. PHI is individually identifiable health information that relates to 1) the past, present, or future physical or mental health, or condition of an individual; 2) the provision of health care to an individual; or 3) payment for the provision of health care to an individual.

Gramm Leach Biley Act (GLBA)

Pursuant to Federal laws, the University of Miami has a duty to protect all nonpublic, personally identifiable financial information. Examples of nonpublic 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 Education Rights and Privacy Act (FERPA)

Family Educational Rights and Privacy Act (FERPA) 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 an 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 (Payment Card Industry Data Security Standard) 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 (IP)

Intellectual Property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. IP 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 IP system aims to foster an environment in which creativity and innovation can flourish.

Last Revision: 05/07/2015