UF UNIVERSITY of FLORIDA

Information Technology

1 Tigert Hall
PO Box 113180
Gainesville, FL 32611-3180
352-273-1788
http://www.it.ufl.edu/

Guidelines for Unsupported Operating Systems at the University of Florida

Scope:

The purpose of this document is to provide guidance for University departments that must continue to operate devices running unsupported operating systems in support of the University Mission.

Guidelines:

Option 1. Turn off the device running the unsupported operating system.

Option 2. Upgrade the device running the unsupported operating system.

Option 3. Disconnect the device running the unsupported operating system from the campus network.

Option 4. Purchase extended support, maintenance and security updates from the vendor.

Option 5. Migrate the device running the unsupported operating system into the designated secure UFNet3 Environment (ISN as of writing this document).

Note: Irrespective of the currency of the operating system (micro code level, etc.) special purpose devices should be migrated to the UFNet3 ISN Environment.

Eligibility Requirements for Option #5:

1. The vendor does not supply extended support, maintenance and security updates.
2. The vendor does not provide an upgrade path to a supported operating system.
3. The upgrade path would put an unrealistic financial burden on the University.
4. Disconnecting the device/system/application would have significant impact to the University, faculty, staff, students.

Technical Implementation actions for Option #5 (Model 1):

1. The unsupported OS will be migrated into a secure UFNet3 environment.
2. The unsupported OS will only be permitted to communicate with two devices.

    a. UFIT administered and supported special purpose VPN.
    b. UFIT administered and supported File Share located in UFDC.
3. "Special purpose VPN" access will require Multi Factor Authentication.

Technical Implementation actions for Option #5 (Model 2):

1. The unsupported OS will be migrated into a secure UFNet3 environment.
2. The unsupported OS will only be permitted to communicate with two devices.
    a. UFIT administered and supported "Bastion Host" located in UFDC.
    b. UFIT administered and supported File Share located in UFDC.
3. "Bastion Host" access will require Multi Factor Authentication and access to the "special purpose VPN" .
4. The "bastion host" will be subject to regular UF InfoSec Security Scanning and audits.

Technical Implementation actions for Option #5 (Model 3):

1. The unsupported OS will be migrated into a secure UFNet3 environment.
2. The unsupported OS will only be permitted to communicate with the following devices.
    a. UFIT administered and supported special purpose VPN.
    b. UFIT administered and supported File Share located in UFDC, and / or,
    c. Upon risk assessment another approved location.
3. "Special purpose VPN" access will require Multi Factor Authentication.

Application Procedure:

1. Departments must submit a Risk Assessment with UF InfoSec and provide the following information:
    a. Information supporting "Eligibility Requirements" above.
    b. Mid/Long term plan for the device/system/application.
    c. Diagram and technical documents supporting the use of the device/system/application.
2. Once the following information is submitted a Risk Assessment will be conducted. Additional information may be required during the review process. UF InfoSec will contact the department if needed.

Renew Procedure:

1. On an annual basis the device/system/application will be re-evaluated by UF InfoSec via the Risk Assessment procedure.