UF UNIVERSITY of FLORIDA
Information Technology

Policy: Remote Access

Purpose:

The purpose of this policy is to define how the University of Florida controls remote access to university information systems and networks in order to prevent unauthorized use.

Scope:

This policy applies to all methods the university implements to allow remote access to its services, information systems and networks.

Policy:

1. All methods the university provides to offer remote access to services and information systems must be assessed for security, approved, documented and controlled. The university will allow external network access only to approved remote access end points.

2. Remote access methods must employ appropriate security technologies to secure the session, as well as prevent unauthorized usage.

Responsibilities:

1. All members of the University of Florida Constituency are responsible for protecting remote access methods, devices and credentials assigned to them. Users are responsible for maintaining the security of computers and devices used to remotely access university resources.
2. Information Security Managers (ISMs) are responsible for documenting and implementing controls for all remote access methods implemented within their unit. ISMs are also responsible for monitoring of unit-implemented remote access methods for unauthorized use, and taking appropriate action upon discovery of unauthorized use, including notification of the UF Information Security Incident Response Team.
3. The Vice President and Chief Information Officer (CIO) is responsible for approval of remote access methods and resources.

4. The Vice President and Chief Information Officer (CIO) is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

Authority:

UF-1.0102: Policies on Information Technology and Security

References:

NIST 800-53 v3: AC-17, AC-17 enh 2