UF UNIVERSITY of FLORIDA
Information Technology

Standard: Remote Access

Purpose:

To establish usage and documentation requirements for remote access methods used at the University of Florida.

Standard:

1. Firewalls and other technology will be used to restrict Remote Access to only approved Remote Access mechanisms.
2. Approved remote access mechanisms will be registered in the Net Services Database.
3. Web servers that provide service to the public, and do not store or provide access to Restricted Data are approved methods of remote access once registered in the Net Services Database.
4. To be approved, Remote Access mechanisms must include the following technical capabilities:
    a. Allow only identified, authenticated and authorized users to connect.
    b. Provide for strong encryption of traffic.
    c. Audit logs contain sufficient information to establish the following:
        i. Event type (authentication, connection or disconnection)
        ii. Date and time
        iii. User associated with the event
        iv. Remote and local IP addresses
        v. Event success or failure
5. Interconnections to the UF Network require interconnection agreements. Access must be restricted to the minimum necessary to achieve the goals of the interconnection.

6. Documentation of remote access mechanisms includes:

    a. Local and remote end points, and mechanisms intended to enforce connection only by intended end points.

    b. Intended users (based upon role or group) and mechanisms to enforce those restrictions.

    c. What university information systems and data remote users may access, and methods to enforce those restrictions.

    d. Guidance provided to users of appropriate uses of the remote access method.

7. Remote access methods must be monitored for unauthorized use, and signs of unauthorized use promptly reported.

References: