Procedure for Vendor Remote Access to the Alachua County Network

Vendor Accounts and Remote Access Guidelines

All vendors will abide by the following guidelines:

a. The department head of the County department for which the system is installed must approve vendor access prior to deployment.

b. Prior to the installation of any system, vendors must request in written the creation of their unique remote access accounts to the Alachua County ITS Security Manager for approval. Vendors will submit the following information:

    Vendor Organization
    Desired VPN account name
    Name and contact information (phone and email) for the employee associated to the account
    System(s) to be accessed
    Anticipated time window of access required
    Detailed description of the anticipated activities (i.e. maintenance / updates / installations) to be performed

c. Vendors will utilize a unique account for each of their employees accessing the Alachua County network. Vendors will not share access accounts and passwords.

d. The account password will conform, at a minimum, to the requested ITS Strong Password Standard, including the 90 day password expiration policy.

e. Vendors will not login using service accounts.

f. Vendors are responsible to notify in written to the Alachua County Security Manager when an employee no longer needs access to the Alachua County network.

g. All remote access must be authenticated and encrypted through the Alachua County Virtual Private Network (VPN).

h. No vendor account will have administrator or elevated privilege access to the system they support, unless it is approved by the ITS Security Manager or the ITS Director.

i. Vendor accounts will have access only to the systems that they support or maintain and that have been approved by the department head of the County agency involved and ITS. Account specific profiles will be created for VPN access and will only be allowed to access specific devices or systems.

j. ITS will be responsible for enabling/disabling accounts and monitoring vendor access to County networks, applications and systems.

Any violation to the above guidelines will result in immediate termination of the user account and remote access privileges.

Vendor Equipment installed in Alachua County Networks.

a. All vendor equipment installed in the Alachua County Network must comply with security standards established by the Alachua County Security Manager. ITS will seek to eliminate any potential exposure of the County networks resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of the Alachua County networks, data, systems and applications.

b. Vendor must provide separate administrative access account to the Alachua County Security Manager for any equipment installed in the county's network, before equipment is attached to the county network.

Alachua County will quarantine or remove any equipment that does not comply with the equipment security requirements or any equipment that compromises the security of the Alachua County network.