



# XXXXXXX XXXXXXXXXXXX XXXXXX POLICY

ADOPTED BY THE GOVERNING BOARD  
OF THE SOUTH FLORIDA WATER MANAGEMENT DISTRICT: MM/DD/YYYY  
RESOLUTION # 200X-XXXX

DISTRICT CLERK'S OFFICE

---

## **Chapter 130**            **INFORMATION TECHNOLOGY**

### **ARTICLE (TBD)**    **REMOTE ACCESS**

**Division**            N/A

#### **Sec. 130-?1. Scope**

This policy defines the requirements and methods available to remotely access South Florida Water Management District (District) networks and information systems; and the Intranet. Compliance and enforcement of this policy will prevent unauthorized access to District data stores while mitigating the introduction of malicious code into District Information Technology (IT) resources.

This policy applies to all District employees, contractors, vendors and agents with a District-owned or personally-owned computer or workstation used to connect to the District's network. This policy applies to remote access connections used to do work on behalf of the District, including reading or sending email, accessing files, running applications and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

#### **Sec. 130-?2. Objective**

The objective of this policy is to define standards for connecting to the District's network from any remote host. These standards are designed to minimize the potential exposure to District from damages which may result from unauthorized use or access to District computer resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical District data repositories or compromise of the flood control system.

Remote Access Users have no right to privacy when using District IT resources. Additionally, the institution or utilization of passwords or encryption or deletion functions to protect or limit access to District IT resources is not a guarantee of past, present or future confidentiality or privacy. The District may monitor, inspect, review, search, remove, or otherwise alter any information communicated or stored using District IT resources at any time and without notice. In addition, all communications are subject to the public records laws.

#### **Sec. 130-3? Statement of Policy**

The District will allow remote access to District networks and systems for employees and authorized third parties working from external locations to reduce travel cost, increase productivity, and provide for optimal use of District networks and systems. Security measures will be implemented to protect District information and IT resources against accidental or unauthorized modification, destruction, disclosure, or loss. Security measures will also be used to protect District IT resources from inappropriate fraudulent use or other criminal acts.



# XXXXXXX XXXXXXXXXXXX XXXXXX POLICY

ADOPTED BY THE GOVERNING BOARD

OF THE SOUTH FLORIDA WATER MANAGEMENT DISTRICT: MM/DD/YYYY

RESOLUTION # 200X-XXXX

DISTRICT CLERK'S OFFICE

---

## (1) General Provisions:

- (a) Secure remote access must be strictly controlled.
- (b) Remote access will require the use of two factor authentication. District issued RSA tokens is the current two factor standard in use at the District.
- (c) At no time should any District employee provide their login, PIN or email password to anyone, not even family members.
- (d) District employees, contractors, vendors and agents with remote access privileges to the District's corporate network are prohibited from accessing the Internet for personal use.
- (e) District employees, contractors, vendors and agents with remote access privileges to District's corporate network must ensure that their remote access connection is given the same consideration as the user's on-site connection to the District.
- (f) District employees and contractors with remote access privileges must ensure that their District-owned or personal computer, which is remotely connected to District's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- (g) District employees and contractors with remote access privileges to the District's corporate network must not use non-District email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct District business, thereby ensuring that official business is never confused with personal business and making their personal email subject to Public Record laws.
- (h) Routers for dedicated ISDN lines configured for access to the District network must meet minimum authentication requirements of CHAP.
- (i) Configuration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- (j) Frame Relay must meet minimum authentication requirements of DLCI standards.
- (k) Non-standard hardware configurations must be approved by the Chief Information Security Officer (CISO).
- (l) Remote access to the SCADA network will require additional authorization by the Operations Control Staff Director.



# XXXXXXX XXXXXXXXXXXX XXXXXX POLICY

ADOPTED BY THE GOVERNING BOARD

OF THE SOUTH FLORIDA WATER MANAGEMENT DISTRICT: MM/DD/YYYY

RESOLUTION # 200X-XXXX

DISTRICT CLERK'S OFFICE

---

- (m) All hosts that are connected to District internal networks via remote access technologies will be subjected to posture validation in accordance with the current requirements and best practices established by the CISO. The District will require the temporary installation of host validation software to ensure the remote device meets the minimum configuration and security requirements.
- (n) Organizations or individuals who wish to implement non-standard Remote Access solutions to the District production network must obtain prior approval from the District's CISO.

## (2) Acceptable Use:

- (a) District IT resources are the property of the District. They are provided to facilitate communications required to accomplish official District business and as a result should be used primarily for the purposes of conducting bona-fide District business; however the District will permit reasonable incidental use of specified resources. Reasonable incidental use is infrequent and brief personal connection and use of a District resource. No employee shall cause the District to incur costs for incidental personal use. Incidental personal use shall not interfere or otherwise conflict with District employee's job performance. Incidental use is subject to all District Policies and Procedures and Public Records Laws.

## (3) Physical Security of Assets:

- (a) Hardware and peripheral devices must be kept safe from physical harm including damage, theft, abuse, or loss. The physical location of District IT resources (Hardware and other physical assets) must be adequately designed and constructed to restrict unauthorized access and use (theft, vandalism and sabotage, etc.), prevent damage due to environment factors (such as heat, moisture or electrical charge), or avoid physical damage. Similarly, data reserved for long-term storage on diskettes or hard drives must be protected from loss due to magnetic fields or electrical pulses, in addition to preventing physical damage or loss.

## (4) External Connection Methods and Guidelines:

### (a) Modems

- i. DUN technology (Modem Bank) is presently being discontinued at the District.
- ii. Use of telephone modems installed on District computers are prohibited unless there is specific business need and they are granted an exception by the CISO.
- iii. Fax Machine analog connections are to be used by the fax equipment only! Unauthorized use of the Fax line for connection to a computer modem is strictly prohibited.

### (b) Virtual Private Network (VPN)



# XXXXXXX XXXXXXXXXXXX XXXXXX POLICY

ADOPTED BY THE GOVERNING BOARD

OF THE SOUTH FLORIDA WATER MANAGEMENT DISTRICT: MM/DD/YYYY

RESOLUTION # 200X-XXXX

DISTRICT CLERK'S OFFICE

---

- i. It is the responsibility of Remote Access Users with VPN privileges to ensure that unauthorized users are not allowed access to District internal networks by protecting their computer, passwords, tokens, and accounts.
- ii. VPN user must be authenticated using two-factor authentication such as a token device and password.
- iii. When actively connected to the District networks, the VPN will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
- iv. Dual (split) tunneling is prohibited in the District Computer environment; only one network connection is allowed while a user is connected to the District VPN.
- v. All computers connected to District internal networks via VPN must have an up-to-date anti-virus software which shall be checked by Universal Access Control (UAC) and forwarded to the appropriate site when District Standards are not met. UAC is in the process of being implemented.
- vi. VPN users will be automatically disconnected from District network after twenty minutes of inactivity or immediately if any security policy violation is detected. If disconnected due to inactivity, the user must then logon again to reconnect to the network. Automatic network processes are prohibited from being used to keep the connection open.
- vii. The VPN concentrator is limited to an absolute connection time of 24 hours. After that, the VPN concentrator should require the user to reconnect and re-authenticate to the VPN.
- viii. Users of computers that are not District issued equipment must configure their equipment to comply with District VPN and Security procedures.
- ix. Only District approved and installed VPN clients may be used.
- x. By using VPN technology with personal equipment, users should understand that the District internal network has been extended to include their remote devices. Because of this, the systems are subject to the same rules and regulations that apply to District-owned equipment. User's machines must be configured to comply with District Standards.
- xi. VPN implementations must maintain point-to-point hardware encryption of at least 128 bits.
- xii. VPN implementations must support a hardware address that can be registered and tracked, i.e. a MAC address



# XXXXXXX XXXXXXXXXXXX XXXXXX POLICY

ADOPTED BY THE GOVERNING BOARD

OF THE SOUTH FLORIDA WATER MANAGEMENT DISTRICT: MM/DD/YYYY

RESOLUTION # 200X-XXXX

DISTRICT CLERK'S OFFICE

---

- xiii. VPN Implementation must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS, or a similar product.
- xiv. VPN access must be obtained with District Supervisor or District Management Sponsor approval in support of a demonstrated legitimate business need.
- xv. VPN accounts/access is prohibited from being shared with other users.

## (c) Broadband Access

- i. Broadband connection types are used by remote access users when connecting to the District VPN. These types of connections include but are not limited to wireless networks provided by District, hotels and service providers (T- mobile hotspots, internet Cafes, etc), Sprint AirNet wireless networking cards, and satellite connections (such as DirectPC).
- ii. While broadband connections are a legitimate method for accessing the internet, they also present several security risks. DSL and cable modem connections are "always on" connections. This means that as long as a computer is turned on, it is connected to the Internet. Always-on connections allow computers susceptible to attack at any hour of the day, providing the computer is powered on. The mandatory use of a District authorized Client required when using Broadband Access will help mitigate the risk associated with DSL and modem connections.
- iii. The remote access mechanisms provided by the District VPN must adhere to District timeout guidelines.

## (d) Mobile Device Access

- i. Mobile Computing Devices are any type of device that can move or be moved and is capable of collection, storing, transmitting, or process electronic data or images. Movement in this case refers to the device generally not having a fixed connection to the network. Personal Digital Assistant (PDAs) combines computing, telephone, fax, internet and other networking features.
- ii. Mobile devices such as Blackberries, Palm Treo devices, and PDAs may be provided with access to internal resources at District. These devices should be configured as securely as possible so that in the event of loss or theft, potential compromise of District data is minimized.
- iii. Modern mobile devices contain nearly as much functionality as laptop or desktop computers. They can access many of the same network resources including documents, email, and web resources as a user connected to the internal network



# XXXXXXX XXXXXXXXXXXX XXXXXX POLICY

ADOPTED BY THE GOVERNING BOARD

OF THE SOUTH FLORIDA WATER MANAGEMENT DISTRICT: MM/DD/YYYY

RESOLUTION # 200X-XXXX

DISTRICT CLERK'S OFFICE

---

through other mechanisms such as the VPN. Because of this, mobile devices should follow many of the same guidelines for security as laptop and desktop computers.

- iv. Mobile Device connectivity must be accomplished through the IT Systems Administration Group responsible for support of these devices. Currently, these mechanisms include corporate email access from Blackberry devices, Palm Treo devices and Personal Digital Assistants.
- v. Mobile devices should receive updates and security patches from the operating system vendor. This must occur on a regular basis as necessary to prevent operating system patches from becoming out of date or vulnerable to attacks.
- vi. Mobile devices should use encryption capabilities to protect data stored on the device.
- vii. If application-level firewall package is available, it should be installed and activated on mobile devices.
- viii. Mobile devices that are lost or stolen must be reported immediately to the IT System Administration Group so that actions may be taken to minimize potential risk.

## (e) Wireless Access

- i. District Wireless Access for employees and contractors is allowed for accessing the District's Enterprise Network, Internal systems, Internet, and Intranet using District laptops which have been loaded with the District Standard firewall, anti-virus and odyssey pc client software to enhance computer security and to direct Internet access through the District's Enterprise Network.
- ii. Public Wireless Access for contractors, vendors, partners, and the general public is allowed for accessing the "internet only". This wireless access does not traverse the District's Enterprise Network. District Contract employees are allowed to use the Public Wireless Access to the "internet only" to communicate with their employers for business purposes only. The District assumes no liability for use or the security of this service. Users of this service are encouraged to have an up-to-date firewall and antivirus loaded and operational on their non-District laptop.

## (f) Internet Service Providers (ISP)

- i. District Employees and contractors may also access their District e-mail by using their personal IPS and accessing <https://exmail.sfwmd.gov>. All applicable District Policies and Procedures apply to this access.



# XXXXXXX XXXXXXXXXXXX XXXXXX POLICY

ADOPTED BY THE GOVERNING BOARD

OF THE SOUTH FLORIDA WATER MANAGEMENT DISTRICT: MM/DD/YYYY

RESOLUTION # 200X-XXXX

DISTRICT CLERK'S OFFICE

---

## (5) Remote Access Methods for Internal Systems:

- (a) Connections required for systems outside of the District's perimeter firewall must be accessed using a secure connection facility, with a suitable form of encryption to secure the connection. Examples of suitable mechanisms include SSH2, SSL, or Triple-DES encrypted Remote Desktop Protocol (RDP).
- (b) Connections required for systems outside of the District's perimeter firewall must be accessed using a secure connection facility, with a suitable form of encryption to secure the connection. Examples of suitable mechanisms include SSH2, SSL, or Triple-DES encrypted Remote Desktop Protocol (RDP).
- (c) Remote administration of routers, switches or other critical network attached appliances shall be accomplished using router software containing a version of the SSH server for remote administration of these devices. Telnet shall not be used and is no longer authorized for network appliance management. Whenever available the SSH2 protocol should be leveraged for remote network device administration.
- (d) Mission critical systems (e.g., SCADA, router systems, windows domain controllers), management or administrative access must only be allowed through secure (i.e. encrypted) sessions.

## **Sec. 130-?4. Policy Violations**

Employees may be subject to disciplinary action up to and including separation from employment for violating this policy or any other District policy or procedure.

## **Sec. 130-?5. Responsibilities**

The Executive Director is charged with the overall responsibility for ensuring compliance with this policy. The Executive Director can designate this authority to the Chief Information Officer. The Executive Director, or the CIO if authorized, shall designate staff to administer this policy. Administration includes, but is not limited to, the design and implementation of procedural guidelines and the management of this policy on a day-to-day basis.

## **Sec. 130-?6. Policy Administration**

The Chief Information Officer or his/her designee will administer this policy and all related IT Security procedures.