

## Virtual Private Network (VPN) Policy

### 1. Purpose

The purpose of this policy is to provide guidelines for Remote Access **Virtual Private Network (VPN)\*** connections to the Miami County Government **network.\*** (\* see Definitions section)

### 2. Scope

This policy applies to all MIAMI COUNTY employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Miami County Government network. This policy applies to implementations of VPN that allow direct access to the Miami County Government network from outside the Miami County Government network.

### 3. VPN approval

- a. Approved MIAMI COUNTY employees and authorized third parties (vendor support, etc.) may utilize the benefits of a VPN, which is a "**user managed**" service.\* part time employees are NOT eligible to use VPN services. (Hourly employees requesting VPN should discuss documentation of "work-at-home" hours with their supervisor and consult the Personnel Policy Manual as appropriate.)
- b. VPN profiles will be created only at the request of Miami County Commissioners and employees manager (MIAMI COUNTY employee's and temporaries), or departmental representative (contractors, consultants, and vendors) by submitting the appropriate [VPN Access Request form](#). Additionally, the user must have read, understood, and acknowledged this policy before using the VPN service.
- c. VPN profiles for non-MIAMI COUNTY personnel (customers, vendors, etc.) must be approved by the Miami County Commissioners and the Information Technology Director. Additionally, a copy of the VPN Request Form (including VPN Policy, and the confidentiality agreement) must be signed by the designated company Approving Authority and filed with the Miami County Auditor's office. Accounts will not be issued until this process has been completed.
- d. VPN profiles are typically created in 2-4 days. Multiple requests may take longer to process. Urgent requests will be reviewed on a case-by-case basis.

### 4. VPN user responsibilities

- a. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the MIAMI COUNTY network, and as such are subject to the same rules and regulations that apply to MIAMI COUNTY owned equipment, i.e., their machines must be configured to comply with all MIAMI COUNTY security policies.
- b. All computers connected to Miami County Government networks via VPN must use up-to-date virus-scanning software and virus definitions. Use of anti-virus software other than Kaspersky must be approved for use by the MIAMI COUNTY Information Technology Director. Additionally, all relevant security patches must be installed; this includes personal computers.

- c. Users of this service are responsible for the procurement and cost associated with acquiring basic Internet connectivity, and any associated service issues. VPN services work best over broadband connections (cable modem or DSL). Use of dial-up Internet service is not recommended for regular VPN activity.
- d. It is the responsibility of the employee or company with VPN privileges to ensure that unauthorized users are not allowed access to Miami County Government networks.
- e. VPN access is controlled using ID and password authentication. For MIAMI COUNTY employees the ID must be in the form of their MIAMI COUNTY email/network ID. For non-MIAMI COUNTY employees the ID will be assigned by the Information Technology office. The password must comply with the MIAMI COUNTY Password Policy. Each VPN user must have a unique profile. Shared profiles are not permitted.

## 5. VPN restrictions

- a. MIAMI COUNTY VPN services are to be used solely for MIAMI COUNTY business and/or support purposes. All users are subject to auditing of VPN usage.
- b. When actively connected to the Miami County Government network, the VPN will force all traffic to and from the remote node through the VPN tunnel. To prevent potential 'back-doors' to the network dual (split) tunneling is NOT permitted. Only one network connection is allowed per VPN session.
- c. Miami County Government network access for non-MIAMI COUNTY personnel will be limited to the resources to which they need access. Open access for these accounts will not be permitted. Additionally, VPN tunnels made to MIAMI COUNTY must contain access restrictions at the remote termination point of the tunnel that prevent unauthorized access to the Miami County network. Tunnels should not be accessible by unauthorized users or the Internet.
- d. All VPN gateways on the Miami County network will be set up and managed by MIAMI COUNTY information technology department. IT will provide approved users with appropriate client software.
- e. User created VPN gateways will not be permitted on the Miami County network.
- f. VPN users may be automatically disconnected from the MIAMI COUNTY network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Artificial network processes are not to be used to keep the connection open. User connections to the VPN may be limited to an absolute connection time of eight (8) hours per day.
- g. The first Tuesday of every month between the hours of 5:00am and 7:00am is reserved for regularly scheduled maintenance. VPN service interruption during that time span may not be announced in advance. However, other emergency downtime will be scheduled and announced as needed.

## 6. Definitions

- a. A **Virtual Private Network (VPN)**, uses encryption and tunneling to connect users or branch offices securely over a public network, usually the Internet. Typically, a VPN will be configured to allow an authorized user to obtain remote desktop control of his/her office system. In the absence of a user controlled system on the Miami County network,

permissions will be configured only for remote access to the systems for which the user has prior authorized access.

- b. **“User managed” service** means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing any required software on their personally owned remote access device (computer, laptop, palm device, etc.).
- c. **Miami County network** refers to the interconnected local and wide area networks maintained and managed by the MIAMI COUNTY Information Technology group.

#### 7. Enforcement

This policy regulates the use of all VPN services to the Miami County Government network. To maintain security, VPN services will be terminated immediately if any suspicious activity is found. Service may also be disabled until the issue has been identified and resolved. Any MIAMI COUNTY employee found to have intentionally violated this policy might be subject to disciplinary action, up to and including termination of employment. Non-MIAMI COUNTY employees and vendors are directly responsible for damage as a direct result of policy violation. Intentional and non-intentional violation will result in termination of service and may result in revocation of contract.

#### 8. Revision history and source

Ver. 1.0, January 31, 2011, Miami County Information Technology office