

## **SECTION 410: VIRTUAL PRIVATE NETWORK (VPN) POLICY**

**410.1 POLICY:** The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the Black Hawk County network. These guidelines are designed to minimize the potential exposure to Black Hawk County from damages which result from unauthorized use of Black Hawk County resources.

**410.2 SCOPE:** This policy applies to all Black Hawk County employees, vendors, contractors as well as all personnel affiliated with third parties utilizing VPNs to access the Black Hawk County network.

### **410.3 PROCEDURES/REQUIREMENTS:**

Approved Black Hawk County employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Additionally, it is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Black Hawk County internal networks.

VPN use is to be controlled using a secured user id and password.

VPN gateways will be set up and managed by Black Hawk County Information Technology Staff.

All computers connected to Black Hawk County internal networks via VPN or any other technology must use anti-virus software identified as the county standard. This includes personal computers and mobile devices. Additionally, all relevant security patches must be installed.

VPN users will be automatically disconnected from Black Hawk County's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

Users of computers that are not Black Hawk County owned equipment must configure the equipment to comply with Black Hawk County's VPN and Network policies. Employees who are accessing protected health information must use County-owned equipment and also comply with Black Hawk County's HIPAA policies and procedures.

By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Black Hawk County's network, and as such are subject to the same rules and regulations that apply to Black Hawk County's owned equipment, i.e., their machines must be configured to comply with Black Hawk County security standards.

## Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a Black Hawk County network must adhere to the following:

- Enable WiFi Protected Access PreShared Key (WPA-PSK, EAP-FAST, PEAP, or EAP-TLS)
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on wireless client and wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

All users are subject to auditing of VPN usage.

This policy regulates the use of all VPN services to the Black Hawk County network. To maintain security, VPN services will be terminated immediately if any suspicious activity is found. Service will also be disabled until the issue has been identified and resolved. Intentional and non-intentional violation may result in termination of service.

Data stored on the network will not be available during system backups as well as any system maintenance.

Any employee found to have violated this policy is subject to disciplinary action, up to and including termination of employment.

### 410.4 DEFINITIONS:

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

**“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.).

**Network** refers to the interconnected local and wide area networks maintained and managed by the Black Hawk County Information Technology department.