

# Remote Access Policy

## **Policy:**

To establish guidelines and define standards for remote access to Kewaunee County's information resources. Remote access is a privilege, and is granted only to remote users who have a defined need for such access, and who demonstrate compliance with Kewaunee County's established safeguards which protect the confidentiality, integrity, and availability of information resources.

## **Responsible for Implementation:**

Security Officer

## **Applicable To:**

All users who work outside of the Organization's environment, who connect to the organization's network systems, applications and data, including but not limited to applications that contain ePHI, if applicable, from a remote location.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

## **Purpose:**

The purpose of this policy is to establish uniform security requirements for all authorized users who require remote electronic access to Kewaunee County's network and information assets. The guidelines set forth in this policy are designed to minimize exposure to damages that may result from unauthorized use of Kewaunee County's resources and confidential information.

## **Scope:**

This policy applies to all authorized system users, including members of the workforce, business associates, and vendors, desiring remote connectivity to Kewaunee County's networks, systems, applications, and data. Users are frequently categorized in one of these user groups:

1. **Workforce members with permanent remote access.** These users are often Information Services (IS), executive, or specific administrative staff, business staff, providers, or teleworkers who require 24-hour system availability and are often called

upon to work remotely or who travel often. Their remote access offers the same level of file, folder and application access as their on-site access.

2. **Workforce members with temporary remote access.** These users typically request short-term remote access due to an extended time away from the office most frequently as a result of a short-term medical or family leave. Access for these users is typically restricted to only that which is necessary for task completion during time away from the office and may be limited.
3. **Contractors and Vendors offering product support with no access to PHI.** These users have varied access depending upon the systems needed for application or system support, but do not have access to any PHI in the applications or systems. These users access the system on an as needed, or as called upon basis for system troubleshooting.
4. **Contractors and Vendors offering product support and other Business Associates with access to PHI.** These users have varied access to PHI depending on the application or system supported and/or accessed. Appropriate Business Associate Agreements must be on file prior to allowing access, and all such access must be audited on a regular basis.

#### **Key Definitions:**

**Defined Network Perimeter.** Refers to the boundaries of the Kewaunee County's internal computer network.

**Electronic Protected Health Information (ePHI).** Protected health information means individually identifiable health information that is: transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

**Firewalls.** A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. A firewall is a set of hardware and/or related programs providing protection from attacks, probes, scans and unauthorized access by separating the internal network from the Internet.

**Information Resources.** Networks, systems, applications, and data including but not limited to, ePHI received, created, maintained or transmitted by the Kewaunee County.

**Protected Health Information (PHI).** Individually identifiable health information that is received, created, maintained or transmitted by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual;
- The provision of health care to an individual;
- The past, present, or future payment for the provision of health care to an individual.

Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.

**Privileged Access Controls.** Includes unique user IDs and user privilege restriction mechanisms such as directory and file access permission, and role-based access control mechanisms.

**Remote Access.** Remote access is the ability to gain access to Kewaunee County's network from outside the network perimeter. Common methods of communication from the remote computer to Kewaunee County's network includes, but is not limited to, Virtual Private Networks (VPN), web-based Secure Socket Layer (SSL) portals, and other methods which employ encrypted communication technologies.

**Role-Based Access.** Access control mechanisms based on predefined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned a predefined role based on the least-privilege principle.

**Teleworker.** An individual working at home (or other approved location away from the regular work site) on an established work schedule using a combination of computers and telecommunications.

**Virtual Private Network (VPN).** A private network that connects computers over the Internet and encrypts their communications. Security is assured by means of a tunnel connection in which the entire information packet (content and header) is encrypted. VPN technology should use accepted standards of encryption, based, for example, on FIPS 140-2.

**Web-based Portal.** A secure website offering access to applications and/or data without establishing a direct connection between the computer and the hosting system. Web-based portals most often use 128-bit or higher SSL encryption.

**Workforce Member.** Workforce means employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

### **Procedures:**

#### 1. Gaining Remote Access

- (a) Remote access is strictly controlled and made available only to workforce members with a defined business need, at the discretion of the workforce member's manager, and with approval by the Security Officer or designee.
- (b) The workforce member is responsible for adhering to all of Kewaunee County's policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for Kewaunee County.
- (c) Business associates, contractors, and vendors may be granted remote access to the network, provided they have a contract or agreement with Kewaunee County which clearly defines the type of remote access permitted as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by the Security Officer and/or legal department before remote access will be permitted. Remote access is strictly controlled and made available only to business associates and vendors

with a defined business need, at the discretion of and approval by the Security Officer or designee.

- (d) It is the remote access user's responsibility to ensure that the remote worksite meets security and configuration standards established by Kewaunee County. This includes configuration of personal routers and wireless networks

## 2. Equipment, Software, and Hardware

- (a) Kewaunee County will not provide all equipment or supplies necessary to ensure proper protection of information to which the user has access.
- (b) Remote users will be allowed access through the use of Kewaunee County equipment or through the use of the workforce member's personal computer system provided it meets the minimum standards developed by Kewaunee County.
- (c) Remote users utilizing personal equipment, software, and hardware are:
  - 1. Responsible for remote access. Kewaunee County will bear no responsibility if the installation or use of any necessary software and/or hardware causes lockups, crashes, or any type of data loss.
  - 2. Responsible for remote access used to connect to the network and meeting Kewaunee County requirements for remote access.
  - 3. Responsible for the purchase, setup, maintenance or support of any equipment not owned by or leased to Kewaunee County.
- (d) Continued service and support of Kewaunee County owned equipment is completed by IT workforce members. Troubleshooting of telephone or broadband circuits installed is the primary responsibility of the remote access user and their Internet Service Provider. It is not the responsibility of Kewaunee County to work with Internet Service Providers on troubleshooting problems with telephone or broadband circuits not supplied and paid for by Kewaunee County.

## 3. Security and Privacy

- (a) Only authorized remote access users are permitted remote access to any of Kewaunee County's computer systems, computer networks, and/or information, and must adhere to all of Kewaunee County's policies.
- (b) It is the responsibility of the remote access user, including Business Associates and contractors and vendors, to log-off and disconnect from Kewaunee County's network when access is no longer needed to perform job responsibilities.
- (c) Remote users shall lock the workstation and/or system(s) when unattended so that no other individual is able to access any ePHI or organizationally sensitive information.
- (d) Remote access users are automatically disconnected from the Kewaunee County's network when there is no recognized activity for 30 minutes.
- (e) It is the responsibility of remote access users to ensure that unauthorized individuals do not access the network. At no time will any remote access user provide their user name or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.
- (f) Remote access users must take necessary precautions to secure all of Kewaunee County's equipment and proprietary information in their possession.

- (g) A firewall shall be used and may not be disabled for any reason.
- (h) Copying of confidential information, including ePHI, to personal media is strictly prohibited, unless the organization has granted prior approval in writing.
- (i) Kewaunee County maintains logs of all activities performed by remote access users while connected to Kewaunee County's network. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity. Inactive accounts will be disabled.
- (j) Electronic Data Security
  1. Transferring data to Kewaunee County requires the use of an approved connection to ensure the confidentiality and integrity of the data being transmitted. Users may not circumvent established procedures when transmitting data to the Kewaunee County.
  2. Users may only send ePHI in a manner approved by Kewaunee County.
- (k) Paper document security
  1. Remote users are discouraged from using or printing paper documents that contain PHI.
  2. Documents containing PHI must be shredded before disposal.

4. Enforcement

- (a) Remote access users who violate this policy are subject to sanctions and/or disciplinary actions, up to and including termination of employment or contract.
- (b) Remote access violations by Business Associates and vendors may result in termination of their agreement, denial of access to the Kewaunee County's network, and liability for any damage to property and equipment.