# Network Access Policy

## Overview

[LEP] data systems are provided as a central resource for [LEP] staff and their customers. It is important that the network infrastructure continues to develop with sufficient flexibility and security while at the same time remaining capable of exploiting anticipated developments in high speed networking technology allowing expanded user services. As additional methods and approaches develop to access network resources, so must related access and management strategies to protect the network from unauthorized use.

2. Purpose

The purpose of this policy is to establish rules for accessing and using [LEP] network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of [LEP] Confidential Information and Personally Identifiable Information (PII).

## Scope

This policy applies to all [LEP] staff who create, manage, deploy, or support network resources within [LEP].

## Policy

### GENERAL

Authorized users are permitted access only to approved [LEP] resources and systems. Users inside the [LEP] firewall may not connect to the network if they are using a wireless connection to connect to an external network.

[LEP] staff and users not involved directly in information security systems management shall not:

* Extend or re-transmit [LEP] network services by installing a router, switch, hub, or wireless access point on any [LEP] administered network
* Install any network hardware or software that provides network services without the express authorization of the [Insert Appropriate Role] or their designee
* Alter network hardware in any way
* Download, install, or run security programs or utilities that reveal weaknesses in the security of a system unless authorized by management
* Run password cracking programs, packet sniffers, network mapping tools, or port scanners

### MANAGEMENT RESPSONSIBILITIES

The [Insert Appropriate Role] or their designee shall ensure procedures and controls exist that maintain and manage:

* Authorization and/or supervision of employees who work with sensitive information in locations where it might be accessed
* Job descriptions that determine appropriate levels of access to sensitive information
* Access to sensitive electronic and paper information
* Employee access to sensitive information and the procedures are organizationally consistent
* Technical safeguards enabling the ability to manage sensitive information and protect against unauthorized access
* Access to sensitive information through a workstation, device, transaction, program, or process
* The manner in which sensitive job functions are performed and the physical attributes of devices that access sensitive information
* Identification and classification of devices that access sensitive information
* Workstation placement and position to only allow viewing by authorized individuals, including specification of additional security measures (e.g. privacy screens, password protected screen savers, auto logoff, etc.) to protect workstations with sensitive information
* Device use for users that access sensitive information from remote locations
* Application sessions termination after a specified period of inactivity
* Automatic logoff shall be implemented on all [LEP] devices capable of this function
* Utility programs that might be capable of overriding system and application controls

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of [LEP] processes. Examples of suitable controls include:

* Regular and documented communications supporting execution of this policy
* Departmental procedures supporting policy
* Computerized logs where appropriate
* Implemented computerized group policy supporting access control and security
* Regular calendars supporting review, testing, and assessment of network access strategies

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 10/28/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |