

# 9400-P174: Network Connections and Management

## I. PURPOSE

This policy provides high-level security requirements to govern how communication and information technology (IT) resources shall be connected to one another to form agency networks and ultimately connect to the State of Wyoming wide area network.

## II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as "agencies"). This policy applies to all wired or wireless networks.

## III. POLICY

- A. For all networks owned and/or managed by the State or one of its agencies, the following apply:
  1. No network or network device, computer system, or modem shall be installed or connected to a network without the prior approval of the agency IT staff. All wireless networks connected to the State WAN shall be also approved by A&I ITD.
  2. Any person creating or opening an unauthorized connection to a network owned, managed, or operated by the State or any of its agencies may be subject to State and Federal criminal prosecution and penalties as well as civil penalties. (Refer to Policy 1200-P142: User Responsibilities.)
  3. Each network segment shall be configured so that it does not increase the risk posed to other network segments. Access controls shall be implemented between segments as necessary.
  4. Each network segment shall be configured to protect the information that it transmits according to the sensitivity and criticality of that information, in accordance with Policy 8100-P131: Information Classification. Whenever possible, an encryption protocol shall be used to protect restricted information transmitted over an agency or State network.
  5. Security controls shall be used for administrative access to a network device or computer system that is connected to a network. Administrative access from a public or uncontrolled network to a State owned or managed network shall not be permitted unless such access is essential to business operations. In all such cases, encryption shall be used for remote administrative connections.
  6. Any device or computer system that is connected to the state network:

## 9400-P174: Network Connections and Management

- a. shall be required to have user and system access controls in accordance with Policy 9400-P170: User Access Management. The ability to identify individuals across network connections shall be retained;
  - b. shall be configured so that it does not reveal information about the device or system, or about the network architecture, except to the extent that such information is necessary to the operation of the network, device, or system;
  - c. shall be configured so that it does not permit unauthorized access to the device or system
  - d. shall be configured so that it does not permit anonymous access to the device or system, except to the extent that such access is necessary to the operation of or service provided by the device or system;
  - e. shall be configured so that it does not provide network services or permit network connections that are not necessary for the use and operation of the device or system;
  - f. shall be, to the extent possible, configured to record information related to security events to a log;
  - g. shall be configured to reduce the risk that the device or system will be compromised, and software patches or firmware updates related to security shall be applied to a device or system in a timely manner, in accordance with best practices and Policy 9400-P183: Technical Vulnerability Management;
  - h. should be configured such that, in the event of a software or hardware failure, the device or system does not increase the risk posed to other devices or systems, or to the networks to which the device or system connects;
  - i. shall be tested to ensure compliance with this and other applicable security policies in accordance with Policy 9400-P211: Policy and Technical Compliance;
7. Before a network device or computer system is connected to a network, or before a change is made to a device or system that may change its security characteristics, that connection or change shall be assessed for unacceptable risks. Agency heads or their delegates shall determine whether risks are acceptable for configurations within their agencies. Department of Administration and Information (A&I), Information Technology Division (ITD) shall be responsible for determining the appropriateness of risk when the State Wide Area Network is involved. A&I ITD shall determine the acceptability of risk when there is a perceived conflict between risks to the State Wide Area Network and an agency's assessment of risk.

## 9400-P174: Network Connections and Management

8. Configuration changes to a network device or computer system shall be reviewed by the agency IT staff to ensure that changes are consistent with this and other security policies such as Policy 9400-P180: Security in the System Lifecycle.
  9. To the extent possible, configuration information, physical location, contacts, and related information about each network device or computer system connected to a network shall be documented and maintained. A diagram for each network, indicating at a minimum every access control device that defines the network perimeter, shall be created and maintained. All such information shall be protected as Restricted information in accordance with Policy 8100-P131: Information Classification.
  10. A computer system affecting the confidentiality, integrity, and/or availability of the State Wide Area Network must be immediately disconnected. Agencies shall be notified when any of their systems are disconnected from the State Wide Area Network and the reason for the disconnection.
  11. All networks, network devices, and computer systems shall be tested to ensure compliance with Policy 9400-P211: Policy and Technical Compliance and any other applicable policies.
- B. In addition to A above, the following shall apply to all wireless networks owned and/or managed by the State or one of its agencies:
1. Wireless networks and connections to the state network shall be encrypted end to end. If an exception is granted for an unencrypted wireless network, the network must provide users with a warning that the network traffic is unencrypted.
  2. Each wireless network shall comply with approved wireless configuration standards and not increase the risk posed to other networks (wired or wireless). Access controls shall be implemented between wireless networks and connected networks.
  3. Any wireless device or wireless computer system connected to the state network:
    - a. shall be configured to protect the information transmitted according to the sensitivity and criticality of that information, in accordance with Policy 8100-P131: Information Classification.
    - b. shall be required to have user and system account accesses in accordance with Policy 9400-P170: User Access Management. Individual accountability shall be retained across network connections.

## 9400-P174: Network Connections and Management

- c. shall be configured so that it does not reveal information about the device or system, or about the network architecture, except to identify the SSID or network by name
  4. Secure mechanisms (such as SSH, SSL/TLS, VPN or others) shall be used for administrative access to a State owned wireless network device or computer system that is connected to a wired or wireless network.
  5. Administrative access from a public or uncontrolled network to a State owned or managed wireless network shall not be permitted unless such access is essential to the operation of the device or system; in all such cases, an encryption protocol shall be used for administrative connections.
  6. Wireless networks shall broadcast their SSIDs. All wireless access points will follow a SSID naming convention standard. (A naming convention standard will be forthcoming.)
- C. For all network connections with public or uncontrolled networks:
1. Each connection between a network owned and/or managed by the State or one of its agencies and a public or uncontrolled network shall be authorized before it is implemented, and shall undergo a risk assessment. Agency heads shall determine if the risks associated with public or uncontrolled networks are acceptable for their agencies. A&I ITD shall be responsible for determining the appropriateness of risk when the State network is involved.
  2. Other than devices used for authorized and risk assessed connections stated above, no device shall bridge a public or uncontrolled network to a State owned network.
  3. While a state or agency computer system is directly connected to a public or uncontrolled network (hotel room, kiosk, home network), follow-on or subsequent connections to State owned networks must be through SSH, SSL/TLS, VPN or other secure mechanism.
- D. For all access control devices:
1. shall be configured to prevent unauthorized access.
  2. shall be configured such that network traffic can be limited, in whole or in part, in order to contain a security incident in accordance with Pending Policy 9400-P191: Security Incident Response and Management.
  3. shall prevent unauthorized connections between distinct development, test, and production computing environments.

## **9400-P174: Network Connections and Management**

4. shall be configured such that any network service that is not specifically permitted between networks is denied, whenever technically possible.
5. shall be limited to the least access necessary in order to meet the business requirements of the service, whenever technically possible.

**CIO Approved Date: 02/01/2010**