1.0 PURPOSE

The purpose of this policy is to provide guidelines to ensure that the Department of Public Safety's (DPS) information technology resources are adequately controlled and monitored.

2.0 POLICY

It is the policy of the Department of Public Safety to control and monitor its information technology resources.

3.0 APPLICABILITY

This policy applies to all DPS employees and contractors.

4.0 REFERENCES

A. NMAC 1.12.6, Architectural Configuration Requirements (ACR)

B. NMAC 1.12.8, Notification of Internet Protocol Addresses

C. NMAC 1.12.11, Enterprise Architecture

D. S-STD-002.001, ACR Configuration Management Standard

E. S-STD-005.001, ACR Network Security Standard

F. N-STD-004.001, ACR Firewall Functionality Standard

G. N-STD-008.1, ACR Wireless Access Point Hardware

H. FBI CJIS Security Policy v4.2

5.0 DEFINITIONS

A. Access (1) – The ability or right to approach, enter, exit, or communicate with or make use of a resource or an area containing a resource.

B. Access (2) – The process of retrieving data from the network. Access is restricted by permissions that are granted to accounts or groups of accounts to network resources.

C. Account – An object in the network that is used to access resources.

D. Advanced Authentication – An extra layer of security designed to further verify the identity of an account that is trying to access the network. There are several forms of advanced authentication defined by the CJIS security policy, any of which, when implemented with regular authentication, provide the required security for accessing the network. These forms are:

1. Virtual Private Networks
2. Biometric Devices

3. Public Key Infrastructure
4. Smart Cards
5. Token Devices

E. Criminal Justice Information Services Division (CJIS) – A division within the United States Federal Bureau of Investigation (FBI) that is responsible for providing timely information to the FBI and other criminal and non-criminal justice agencies and institutions about law enforcement–related matters.

F. Dissemination – The process of distributing data.

G. Encryption – The process of making data unreadable without the corresponding decryption algorithm. This process can be simple obfuscation or can involve highly complex mathematical formulae.

H. Firewall – Any device that uses a set of rules to provide controlled connectivity between networks of differing zones of trust. Two firewalls can also typically encrypt traffic (see Virtual Private Networks) between them.

I. Network – The communication infrastructure that is used to store and transmit data.

J. Network Device – Any device or component that provides access to or controls the communication infrastructure of the network. This includes, but is not limited to, routers, switches, firewalls, hubs, modems, wireless access points, and remote access devices.

K. Password (Fixed) – A secret set of characters, set by a user, which, in combination with a User ID, grants access to network resources for an account. The procedures in this policy regarding password changes only apply to fixed (set by a user) passwords and not to system-generated, one-time dynamic passwords.

L. Physically Secure Location – Any area that has controlled and monitored access.

M. Privilege – The rights that are granted to an account to perform certain tasks on the network.

N. Remote Access – The process of accessing the network using a public network. This is usually through dial-up, using the Public Switched Telephone Network (PSTN) or through a Virtual Private Network (VPN) using an encrypted path through the Internet.

O. Resource – Any file, folder, network share point, server, or device that contains data or controls the flow of data on the network.

P. User ID – A unique identifier that differentiates one account from another. User IDs are not secret, although they should be treated as sensitive.

Q. Wireless Local Area Network (WLAN) – A network that connects computers and resources over a radio frequency. A WLAN can be used to extend the network to areas for temporary access, where running cable is too expensive or for mobile computer users.

6.0 PROCEDURE

A. Network Administration –

1. GSD shall be notified of any changes to publicly-visible Internet Protocol addresses – refer to: NMAC 1.12.8.8 and 1.12.11.15.

B. Data Communications Security

1. Inter-site and external communications

a. All data transmitted between sites through any public network segment, including radio transmissions and Wireless LANs, shall be protected with a minimum of 128-bit encryption.

b. Connections from external networks to DPS resources must meet all requirements in ACR (ACR – Architectural Configuration Requirements) S-STD-005 section 4.6.

2. Wireless LAN Devices - Refer to State of New Mexico ACR N-STD-008 for all policies and standards regarding WLAN hardware implementation.

3. Firewalls

a. All networks that have access to unprotected or protected external or protected internal networks shall be protected by a firewall.

b. All firewall devices shall be housed in a physically secure location.

c. All firewalls shall permit the minimum amount of access in order to allow the required traffic to pass. The final rule in all firewall devices shall be “Deny All”.

d. Firewall policies shall be reviewed every ninety (90) days.

e. All firewalls shall run on dedicated devices or computers and shall not serve other purposes. Firewall operating system builds shall be based on minimal feature sets. This includes the removal of all unnecessary programs, compilers, and network protocols prior to firewall implementation.

f. All unused user or system accounts, physical network interfaces, and services shall be disabled or deleted.

g. All user and system accounts shall meet the approved DPS password policy.

h. All firewalls shall use a minimum of two network interfaces. Firewalls that utilize a single network interface or otherwise conduct inbound and outbound traffic on a single interface are not permitted.

i. The following types of packets/traffic shall always be blocked:

1. Source-routed packets

2. Packets with the IP options field set

3. Any packet with the source or destination set to 127.0.0.1 or 0.0.0.0

4. Directed broadcasts

j. All firewalls that are not part of a high-availability cluster shall fail to a closed state.

k. All firewalls shall have security logging turned on. Firewall logs shall be reviewed on a daily basis and shall be retained for a minimum of one year.

l. All firewall purchases (including sizing and VPN compatibility) must meet the requirements in the State of New Mexico ACR N-STD-004.

C. Configuration Management – This section contains policies that pertain to how changes to the network are to be effected

1. The Department of Public Safety shall maintain a State of New Mexico–approved change management policy according to ACR S-STD-002.

2. All changes to the network including the addition or modification of network devices or communications paths and addition or modifications of servers or software shall go through a DPS-approved life cycle process.

3. All changes to firewalls, in addition to following the standard change management procedure, shall be preceded by a full backup of the firewall. All firewalls must support an audit trail to track changes.

D. Patch Management

1. All computers shall have patches and updates applied through a centralized server (or servers) that provides the ability to approve patches and updates prior to deployment.

2. Server computers shall be approved separately from non-server computers.

3. All patches and updates that are scheduled for deployment shall be tested prior to release. Exceptions can be made for critical updates that impact the security of DPS assets if these exceptions are approved by the DPS Chief Security Officer or his/her designee.

4. DPS administrators shall monitor and address software and firmware vulnerabilities of all network devices by ensuring that applicable updates are acquired, tested, and installed in a timely manner.

E. Virus Protection

1. Virus protection software that is capable of detecting and eliminating viruses shall be employed on all computer workstations, laptops, and servers that are ever connected to the DPS network. This includes all LEA devices.

2. Virus protection software shall be enabled at system start-up and will employ resident scanning and shall not be configurable or unloadable by end users.

3. Virus protection software on all computer workstations, laptops, and servers will be configured to update virus signatures immediately or as soon as possible after release.

F. Systems Monitoring

DPS uses different systems to monitor different types of server and network processes. DPS IT staff will continue to use the best tools to conduct necessary monitoring in order to maintain the highest level of availability and security possible. At a minimum, the following shall be monitored:

1. Server Monitoring

   a. Events: Event logs from all servers shall be collected centrally. These event logs shall be reviewed at least a weekly.

   b. Services: Services and daemons shall be monitored continuously. Notifications for stopped services shall be sent to appropriate IT staff in the event of a malfunction.

2. Network Monitoring

   a. Performance: Performance for critical network devices shall be monitored continuously.

   b. Intrusion Detection/Prevention: An intrusion prevention or intrusion detection system (IDS/IPS) shall monitor secure network segments continuously.

G. Administrative Access

1. No regular user account shall be given administrative privileges on any computer.
2. Network Devices
   a. Access to network devices for administrative purposes must use encryption.
   b. Network Devices shall not share a common logon and password. All network devices must either:
      1. Have a unique logon that is different from all other network devices and from any regular or elevated-privilege account.
      2. Be centrally authenticated.
   c. All devices shall have their vendor-supplied default passwords changed prior to production implementation.

H. Documentation

1. All IT devices (including, but not limited to, computer servers, workstations, laptops, firewalls, network routers, and network switches) shall be recorded in inventory in the Statewide Asset Management System according to State of New Mexico ACR S-STD-002. This shall include all wireless device ID numbers and contact numbers of wireless providers to allow for the deactivation of lost or stolen devices.
2. All network systems will be completely documented and maintained according to State of New Mexico ACR S-STD-002.
3. The words “FOR OFFICIAL USE ONLY” shall appear near the bottom of the page on all documentation.
4. DPS shall maintain the signed copy of all users’ intent-to-comply statements for as long as the user is employed by, has a contract with or otherwise provides services to DPS.

7.0 ATTACHMENTS

NONE

8.0 APPROVAL

APROVED BY: s/John Denko DATE: September 9, 2008
DPS Cabinet Secretary