1.0 PURPOSE

The purpose of this policy is to ensure that risks to the Department of Public Safety's (DPS) Information Technology (IT) resources are minimized and that, in the event of an exposure, proper steps are taken to recover and minimize future impacts from similar threats.

2.0 POLICY

It is the policy of the Department of Public Safety to maintain procedures which provide for the security and recovery of its information technology resources.

3.0 APPLICABILITY

This policy applies to all DPS employees and contractors.

4.0 REFERENCES

A. S-STD010.001, Backups Standard

B. S-STD004.001, Account Management Standard

C. S-POL003.001, Security Training and Awareness

D. STD012.001, Incident Response and Reporting

E. 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. **Asset –** A valuable item (hardware, software, or data) owned/stored by the Department and worth protecting.

F. **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.

G. **Dissemination –** The process of distributing data.

H. **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.

I. **Exploit –** To take advantage of a weakness or vulnerability in a system.

J. **Exposure –** A specific instance of damage to an asset, possibly resulting in the loss of that asset, due to a threat exploiting a vulnerability.

K. **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.

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

M. **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, hubs, modems, wireless access points, and remote access devices.

N. **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 policies in this document regarding password changes only apply to fixed (set by a user) passwords and not to system-generated, one-time dynamic passwords.

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

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

Q. **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.

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

S. **Risk –** The likelihood, expressed as a percentage or a generality (e.g., high, medium, low) of a threat exploiting a vulnerability.

T. **Safeguard –** A specific countermeasure that is used to mitigate a threat agent. Some types of safeguards protect against multiple types of threat agents.

U. **Threat –** A potential danger that, if it successfully exploits a vulnerability, can damage an asset.

V. **Threat Agent –** A specific instance of a threat. For example, a hole in the roof is a vulnerability. There is a risk that water coming through the roof could damage assets inside. A rainstorm, in this case, would be the threat agent.

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

X. Vulnerability – A weakness in the security infrastructure that could be exploited and result in damage to an asset.

Y. 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 or where running cable is too expensive.

6.0 PROCEDURE

A. Audit Trails

1. All systems that authenticate users or protect assets shall support event logging.
2. The following events shall be audited on all systems that support event logging:
    a. User authentication (success/failure)
    b. Remote access attempts (success/failure)
    c. Password changes (success/failure)
    d. File access (success/failure) to protected information
    e. Event log clearing
    f. Privilege elevation
    g. Firewalls must track changes and backups must be retained (n-std004)
3. All systems shall be configured to retain one (1) month of security events on line. After one (1) month, the event logs may be moved into offline storage where they shall be kept for twelve (12) months.
4. All log files shall be protected against unauthorized changes, clearing, or destruction.
5. All systems shall use an automated event log parser with centralized logging, reporting, and notifications.
6. Audit logs shall be reviewed once per week.

B. Business Continuity

1. DPS shall form a Disaster Recovery (DR) team that consists of at least one member from every IT functional area and a team leader shall be named.
2. DPS shall maintain a complete DR manual. This manual shall include procedures for recovering from and supporting the business operations of DPS during the following incidents:
    a. Extended power outage
    b. Equipment theft
    c. Extended communications outage
    d. Partial or complete data center destruction
3. The DPS DR manual shall be reviewed and tested by the DR team every two (2) years to ensure that all current IT and business-related IT operations can survive an incident. These tests shall be documented and the documentation shall be maintained by the DR team for a specific time period as determined by the team.

4. Backup and Restore

   a. DPS shall appoint an individual to be the backup administrator and another to be the alternate backup administrator. The backup administrator (or alternate) shall be responsible for scheduling and monitoring all information systems backups, restoring data upon request, and performing regular tests of the system.

   b. The DPS backup administrator shall maintain a backup and restore manual which shall contain all schedules for all backup groups including the type of backups performed and the schedules for all test restores.

   c. The DPS backup administrator shall maintain a log of all backups and restores performed and the disposition of those backups and restores. This log shall be maintained for one (1) year and will be stored on archival media in physical proximity with the one-year archive.

   d. The DPS backup administrator shall maintain a separate log for all restores (test and production). The format of this log should be such that reports of restores to supervisors can be expedited.

   e. All critical business information and critical software resident on DPS servers shall be periodically backed up according to the schedule above.

   f. Business critical information shall not be stored on workstations. Laptop users will copy business critical information to the server after connecting to the DPS network.

   g. A current copy of all backups shall be maintained in an environmentally-protected and access-controlled location away from the DPS premises at all times.

   h. All information that is recorded on any form of backup computer media that is stored away from DPS premises shall be encrypted or protected by password.

   i. Media that is no longer usable for backup purposes shall be destroyed as specified in departmental policy ADM:31, Access to and Use of Computer-Based Resources.

C. Non-Disclosure and System Access Agreements

1. DPS shall maintain a Non-Disclosure Agreement (NDA) that indemnifies DPS against the accidental or willful release of protected information by non-DPS personnel that have access to protected information. All vendors and external agencies shall sign a NDA.

2. DPS shall maintain a System Access Agreement (SAA) that states that non-DPS personnel will have access to DPS information systems and potentially protected information and agree to be bound by all DPS information systems security policies. All vendors and external agencies that have access to internal DPS information systems shall sign a SAA.

D. Education

1. DPS shall maintain a security awareness training program. This program shall follow the content guidelines specified in SoNM ACR S-POL-003 (approval pending).

2. All employees shall receive security awareness training within three (3) months of employment.

3. All employees shall go through security training within three (3) months of every three (3) year anniversary.

4. All users, as a part of their security education, shall be shown where to store critical business information and the value of backups.

5. The employee shall sign a statement to the fact that security awareness training was received and DPS shall maintain a record of that employee's security awareness training for the duration of that employee's tenure at the Department.

E. Threat Identification

1. Audits

   a. Agency Operational Systems

      1. DPS shall conduct security audits of all Departmental operational systems at least once every three (3) years.

      2. DPS shall conduct quarterly security audits of five (5) systematic local (city and county) law enforcement agencies' operational systems.

   b. DPS shall conduct monthly password audits to ensure that users are conforming to its password policies.

2. Penetration Testing

   a. DPS shall maintain a standardized methodology for testing open services and known vulnerabilities. This shall be known as the penetration test manual and should include:

      1. Tools used

      2. Risk acceptance levels

      3. System and IP address enumeration

      4. Port scans and service offerings

      5. Rogue network device detection (including Wireless Access Points and other consumer-level devices, such as hubs)

      6. Vulnerability tests, including Denial of Service (DOS)

      7. Use of exploits intended to gain access or elevated privilege.

   b. The DPS Chief Security Officer or designee shall conduct regular audits (penetration tests) of the DPS systems and random audits of all local law enforcement agencies that connect to DPS systems. Final reports for each test should include:

      1. All footprint information

      2. Vulnerabilities found

      3. Exploits successfully used

      4. Recommendations for remediation

      5. Penetration tests may be automated and the results shall be retained in a report format for a minimum of two (2) years.

   c. DPS penetration test manuals shall be reviewed yearly to ensure that it is both timely and includes the latest relevant exploits.

F. Incident Response

1. In order to ensure a quick, effective, and orderly response to IT security incidents, the individuals responsible for handling IT security incidents shall be clearly defined.
2. The DPS CSO shall be the Point of Contact (POC) for all IT security incidents.
3. The DPS CSO shall designate a local POC for all interface agencies that connect to the DPS network.
4. DPS shall always have an employee or contractor on staff that is educated in:
   a. Intrusion detection techniques – see S-STD-005 (4.9)
   b. Penetration testing techniques
   c. Computer forensic evidence preservation techniques
5. DPS shall maintain a standardized methodology for intrusion detection/prevention, forensic evidence preservation, and for detecting exposures-in-progress and reporting them to the CSO, or designee. This shall be known as the Incident Response Manual.
6. All IT security incidents shall be reported to the DPS CSO or designee and documented using a standard report.
7. The DPS POC shall notify the FBI CJIS Division Information Security Officer (ISO) and the Computer Security Incident Response Capability (CSIRC) immediately upon discovery of an IT security-related incident that could compromise the security or data integrity of any CJIS system.
8. The DPS POC shall notify the FBI CJIS Division ISO within four (4) hours after the resolution of an IT security-related incident.
9. The DPS CSO or designee shall notify the State of New Mexico Computer Security Incident Response Team (CSIRT) within one hour of detection of an IT security-related incident.
10. The DPS CSO or designee shall complete a State of New Mexico CSIRT Incident Report.
11. The DPS CSO shall provide a copy of the DPS report when notifying the FBI CJIS Division ISO.
12. The DPS shall maintain a contingency plan for recovery from an IT security-related incident that will allow for the disinfection, repair, and upgrade of the affected system(s). This plan shall be routinely reviewed, tested, and updated so that downtime can be kept to a minimum.

7.0 ATTACHMENTS

NONE

8.0 APPROVAL

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