MANAGEMENT DIRECTIVE

245.18
Number

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE

Subject:

IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response Policies and Procedures

By Direction Of:

Joseph S. Martz, Secretary of Administration

Date:

February 7, 2006

This directive provides guidance regarding Information Technology (IT) Administrator security assurance practices.

1. PURPOSE. The purpose of this directive is to provide guidance regarding the ethical and acceptable use of Commonwealth of Pennsylvania (CoPA) information technology (IT) resources by network/system/database administrators, henceforth known as "Administrators." The directive also details the auditing and monitoring procedures that will be employed to ensure that Administrators do not misuse their authority. Finally, this directive establishes a policy for reporting information technology security incidents involving Commonwealth Administrators that may compromise the availability, integrity, and confidentiality of the Commonwealth enterprise infrastructure and information systems.

2. SCOPE. This directive applies to all individuals (e.g, employees, contractors, etc.) in departments, boards, commissions, and councils under the Governor's jurisdiction, who have access to the Internet on CoPA computer resources. Agencies not under the Governor's jurisdiction are strongly encouraged to follow the policy and procedures stated in this directive.

3. DEFINITIONS (These are collectively referred to as central administrators).

a. Database Administrator. A person responsible for the design and management of one or more databases and for the evaluation, selection and implementation of database management systems.

b. Network Administrator. A person who manages a communications network within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program and providing for routine backups.

c. System Administrator. A person who manages the computer systems in an organization. The responsibilities of a system administrator and network administrator often overlap. A system administrator is involved with operating system and hardware installations and configurations and may be involved with application installations and upgrades. A system administrator may also perform systems programmer activities.

d. Enterprise Database/Network/System Administrator. Responsible for the maintenance of computer IT resources shared by CoPA agencies.

e. Agency Database/Network/System Administrator. Responsible for the maintenance of individual agency computer IT resources.

f. Local Database/Network/System Administrator. Responsible for the maintenance of individual workstations owned by a CoPA agency.

4. BACKGROUND. While perimeter security of the CoPA's IT systems remains vital to ongoing operations and business continuity of the Enterprise, internal security must be addressed with the same due diligence. Security cannot and must not reside only at the perimeter of the Enterprise. Internal security encompasses the following:

a. "Security Awareness" communication and training of all Commonwealth employees.

b. Provisioning, de-provisioning and vetting of employee, business partner and citizen access.

c. Identification of internal security risks associated with intentional or inadvertent misuse of granted access to and/or control of content sensitive or mission critical systems and information.

d. Ability to audit and monitor the activities of administrators whom the Commonwealth entrusts to maintain the health and availability of content sensitive and mission critical systems.

5. POLICY. Administrators are required to manage, configure and monitor CoPA IT resources. Administrators also have the ability to create, access, modify and/or delete electronic resources, data and systems configurations within a given technology discipline as well as granting permissions to other individuals commensurate with their own privileges in a given technology discipline. Because administrators are trusted with rights and privileges beyond those granted to normal CoPA system users (users) they must adhere to the highest standards of ethical conduct in the use of and administration of CoPA IT resources. Acceptable use guidelines of CoPA IT resources by administrators can be found in Enclosure 1.

In addition, Administrators will be subject to stringent auditing and monitoring of their activities in order to maintain the highest level of internal security. The auditing and monitoring shall be performed by a security business unit separate from the infrastructure and operations personnel tasked with maintaining the health and security of the enterprise infrastructure. The separation of duties shall be utilized as a measure of avoidance for a potential conflict of interest. This process shall provide validation and confidence of the health and security of the Commonwealth's infrastructure and information systems within the perimeter of the enterprise (See Enclosure 2).

If while Auditing and Monitoring IT administrators an incident is detected, Enclosure 3, Incident Response, Notification, and Escalation Procedures for Security Incidents Involving Commonwealth IT Administrators, must be followed.

6. DISCIPLINE. Because administrators are trusted with rights and privileges beyond those granted to normal CoPA system users, administrators must adhere to the highest standards of professional and ethical conduct in the use of and administration of CoPA IT resources. Failure to protect the integrity or the security of the network, or misuse of administrative authority, is grounds for immediate dismissal.

7. QUESTIONS. Questions pertaining to this policy should be directed to the Bureau of Enterprise Architecture via ra-oaitb@state.pa.us.

Enclosures:

1 – Acceptable Use Policy Agreement for Network/System/Database Administrators
2 – Auditing and Monitoring IT Administrators
3 – Incident Response, Notification, and Escalation Procedures for Security Incidents Involving Commonwealth IT Administrators
4 – Point of Contact Information Template
5 – Incident Response Documentation Template

Acceptable Use Policy Agreement for Network/System/Database Administrators

Acceptable uses of CoPA IT resources by administrators include but are not limited to:

1. Adherence to the standards set forth in *Management Directive 205.34, Standards for Employee and Other Authorized User Internet Use and Electronic Mail Communications*.

2. Performance of activities deemed necessary to support the overall health, availability, integrity and security of:

a. Servers, desktops, and laptops owned or controlled by CoPA.

b. Network and infrastructure systems owned or controlled by CoPA.

c. Physical and electronic security systems owned or controlled by CoPA.

d. Database and application systems owned or controlled by CoPA.

3. Guarding against corruption, compromise, or destruction of CoPA computer and network resources and information assets.

4. Maintaining and applying all system patches and system updates taking into account the expense of applying the patch, the expense of recovering from a failed patch and the likelihood that not applying a given patch will result in a security breach.

5. Taking reasonable and appropriate steps to insure that all hardware and software license agreements are faithfully executed on all systems, networks, and servers.

6. Ensuring agency network addresses are assigned only to those entities or organizations that are part of the agency. Administrators shall not assign network addresses to non-agency entities or organizations without the specific written approval of the agency chief security officer.

7. Limiting access to root, administrative, service or privileged supervisory accounts (privileged accounts) on CoPA computer and network resources to administrators only. Privileged accounts are accounts that have virtually unlimited access to all programs, files, and resources on a computer system. Users shall not be given access to privileged accounts without the specific approval of the agency chief security officer. Privileged accounts must be used only for the purposes for which they were authorized and only for conducting CoPA business.

8. Ensuring that default passwords shipped with servers, operating systems, databases, network equipment, or software applications are changed using strong password methodologies when the resource is installed or implemented.

9. Never sharing personal or privileged account logins or passwords with anyone including other administrators without the approval of the agency chief security officer.

10. Never allowing users to log into computer resources with privileged account access.

11. Performing all regular CoPA activity under a personal account and not through a privileged account.

12. Never knowingly creating pathways that allow for violations of network security.

13. Never gaining unauthorized access to a system (or area of a system) using knowledge of access abilities gained during a previous position at another agency or institution.

14. Never giving access on a system you do not administer to another user.

15. Always logging off or appropriately securing sessions with privileged account access to a point that requires a new log-on whenever leaving your work area.

16. Treating the files of system users as private unless there is reason for suspicion such as hacking, sending illegal material, etc. Administrators routinely monitor and log general usage data. When problems become apparent, they may review this data for evidence of violation of law or policy as directed by the agency security officer. When necessary, they may monitor all the activities and inspect the files of specific users on their computers and networks. If there is reason for suspicion departmental legal counsel and the agency security officer must be contacted before any action is initiated.

17. Respecting the privacy of electronic communication. Administrators shall not obtain/intercept, or attempt to obtain/intercept any electronic communication or information not intended for them unless such activities are performed as part of their authorized job duties. Administrators have the duty to the owners of the information to protect the confidentiality of all such information. This includes making changes to, ensuring unauthorized users do not have access to, or not divulging to a third party that information.

18. Ensuring that all network activities tracked are complete for all users. Administrators may not single out individual users for tracking or logging, unless directed to do so by the agency human resource office and/or agency legal counsel. All users must be tracked or logged equally. To ensure the integrity of procedures and policies of network administration or to ensure network security, additional or extra activities of the administrators may be tracked.

19. Never engaging in any illegal or inappropriate use of CoPA IT resources or engaging in activities that interfere with or disrupt network users, services, or equipment. Illegal use shall be defined as use which violates local, state, or federal law as well as CoPA or agency IT policy. Inappropriate use shall be defined as a violation of the goals, purpose and intended use of the network. This includes, but is not limited to, the following: stalking others, supporting partisan political activities, transmitting or originating any unlawful, fraudulent, defamatory, or obscene communications, or any communications where the message or its transmission or distribution, would constitute or would encourage conduct that is a criminal offense or would give rise to civil liability. Interference or disruption includes, but is not limited to, distribution of unsolicited advertising or mass mailings; “spamming,” propagation of computer worms or viruses.

EMPLOYEE ACKNOWLEDGEMENT.

I have read and understand the acceptable use policy for Network/System/Database Administrators. I will adhere to the established policy and understand if I violate the rules explained herein, I may be subject to disciplinary action, up to and including termination of employment.

Name (Print): ____

Signature: ______________________ Date: ______________________

Auditing and Monitoring IT Administrators

This enclosure outlines the activities that should be monitored by administrators. Please note, the central administrators will not monitor agency administrators. The monitoring of agency administrators is the responsibility of the agency Chief Security Officer. The monitoring of central administrators will be done by the Enterprise Security Counsel and the OIT Information Security Officer.

1. The following is a list of activities that should be monitored by agency and central administrators:

a. Unauthorized access, deletion, creation and/or modification of CoPA's IT systems and data.

b. Unauthorized account creation, modification or deletion.

c. Creation of unauthorized entry or access points into the CoPA's IT systems.

d. Unauthorized transfer or access of data or information within the CoPA's IT systems.

e. Unauthorized transfer or access of data or information outside of the CoPA's infrastructure.

f. Unauthorized use of another individual's identification and password.

g. Malicious attempts to jeopardize the health of the CoPA's IT systems.

h. Attempts to conceal malicious or unauthorized activity.

2. Monitoring the Active Directory Infrastructure. The monitoring (or "health-checking") process gathers information about the security state of the Active Directory® directory service infrastructure, which includes the directory database, domain controllers, and administrative workstations for service administrators. To monitor the Active Directory infrastructure, the following will be performed:

a. Collect information in real time or at specified time intervals.

b. Compare this data with previous data or against a threshold value.

c. Respond to a security alert as directed in your organization's practices.

d. Summarize security monitoring in one or more regularly scheduled reports.

The Commonwealth will leverage monitoring software to collect and interpret this status. In addition, the Commonwealth has numerous domain controllers and administrative workstations, which can best be supported by compiling status information in a common database. After the information is centralized, it can be reviewed to monitor the security status of Active Directory as a whole.

3. Event notification. The monitoring described below is for the purpose of detecting security-sensitive configurations and not for the purpose of detecting intrusions. With event notification, thresholds are defined for changes in the directory service, domain controller configuration, or other Active Directory infrastructure characteristics. When one of these characteristics changes enough to exceed the threshold, an event notification is generated, indicating a potential security breach.

4. Trend analysis. With trend analysis, information is collected as a number of data points that are only meaningful when they are examined over a period of time. Drastic changes in trends can indicate a potential security breach.

a. Monitoring the Active Directory infrastructure will be performed as follows:

(1) Changes to Active Directory.

(2) Changes in domain controller status.

(3) Changes in system state and executables.

Active Directory is an integral component in a domain's security mechanism. A big part of securing Active Directory installations is monitoring security-sensitive changes to Active Directory containers and objects. The security auditing recommendations from Microsoft presented in "Establishing Secure Domain Controller Policy Settings" in Securing Active Directory Installations and Day-to-Day Operations: Part I establishes audit settings for security-sensitive administration tasks and must be in place for you to monitor changes to Active Directory.

b. Monitor changes to Active Directory containers and objects by performing the following tasks:

(1) Monitor forest-level changes.

(2) Monitor domain-level changes.

(3) Monitor changes in the Service Administrators Operational Unit (OU).

(4) Monitor changes to the disk space consumed by Active Directory objects.

5. Monitoring Forest-Level Changes. Forest-level changes in Active Directory have the broadest scope of any administrative operations, and as such they represent a large security attack surface. Forest-wide configuration changes include the following:

a. Changes in the schema.

b. Promotion or demotion of domain controllers, especially global catalog servers.

c. Changes in replication topology, including changes in sites and subnets.

d. Changes in policies for Lightweight Directory Access Protocol (LDAP).

e. Changes in the dSHeuristics attribute.

f. Changes in forest-wide operations master roles.

6. Monitoring Domain-Level Changes. Changes in Active Directory domains affect all users, workstations, member servers, and domain controllers in the domains, and as such they represent a large security attack surface. These domain-wide configuration changes include the following:

a. Changes in domain-wide operations master roles.

b. Changes in trusts.

c. Changes in permissions for Administrators and Domain Admins through modification of AdminSDHolder.

d. Changes in the Group Policy Objects (GPOs) for the Domain container and the Domain Controllers OU.

e. Changes in the GPO assignments for the Domain container and the Domain Controllers OU.

f. Changes in the membership of built-in groups, such as Administrators and Backup Operators.

g. Changes to the audit policy settings for the domain.

Incident Response, Notification, and Escalation Procedures for Security Incidents Involving Commonwealth IT Administrators

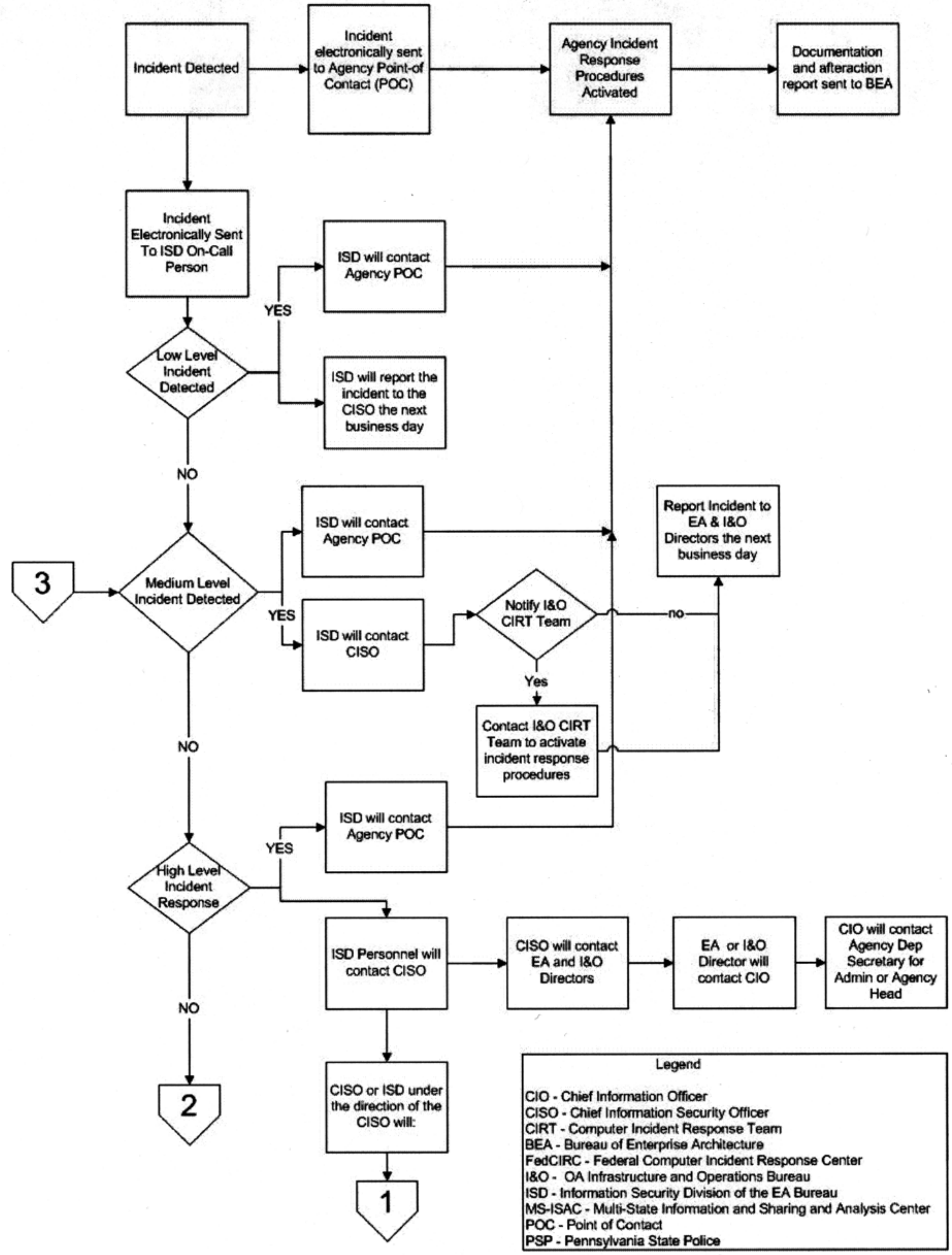
Auditing and monitoring of all Commonwealth administrators shall be performed. In the event that an incident is detected, the following incident escalation and notification process shall be followed.

Incident Level Definition. Incident levels are determined by the business impact of the incident. Business impact is determined by two factors: if the activity is criminal and how much damage the organization reputation will sustain.

Low Level Incident. Impacted resource go no farther than a user work station. Criminal activity is not suspected. Maximum response time for the incident is the next business day.

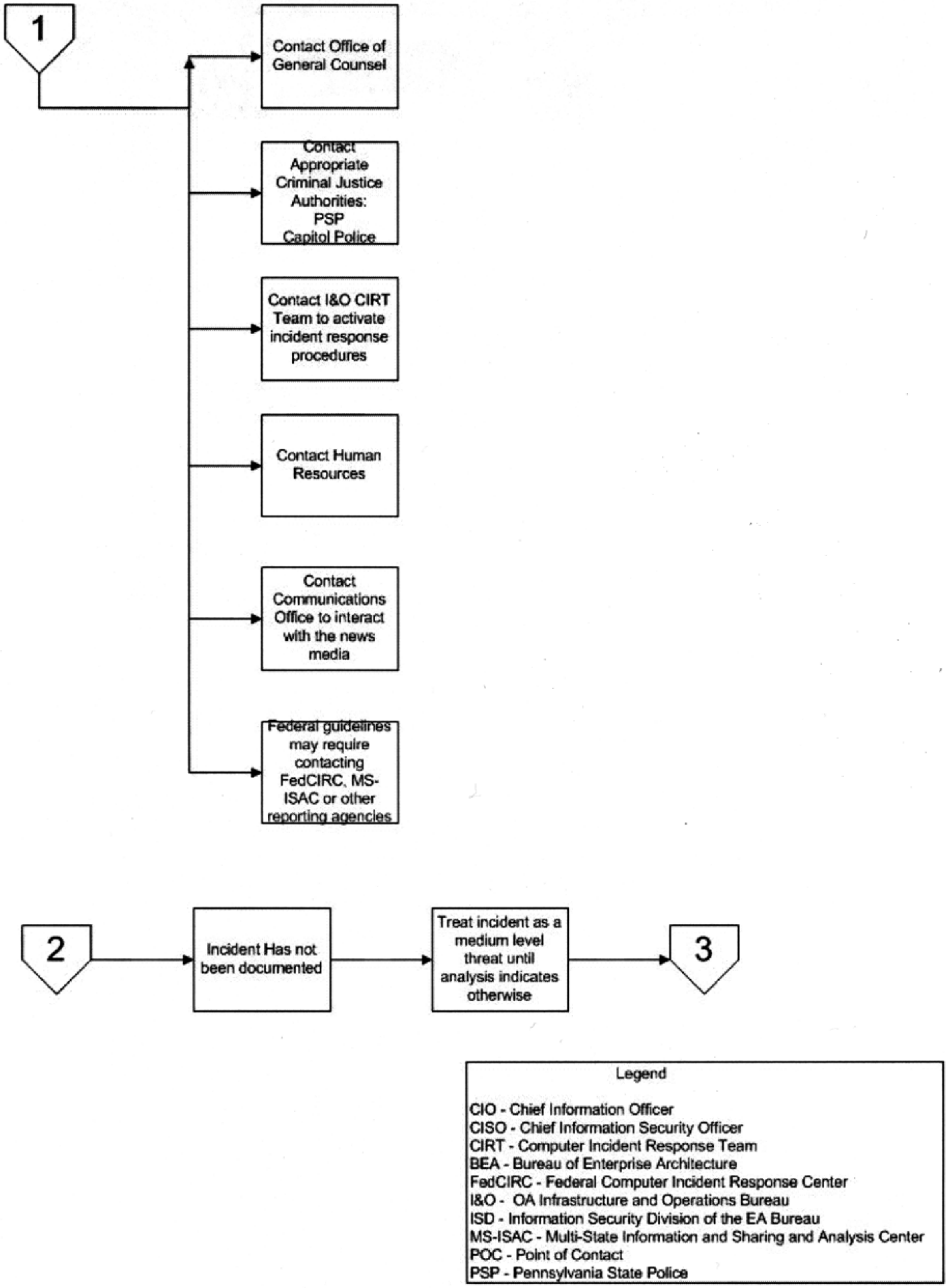
Medium Level Incident. Impacted resources included workstations, file and print servers and application data. Criminal activity is not suspected. Maximum response time for the incident is 4-8 hours.

High Level Incident. Impacted resources include internet connectivity, public web servers, highly critical system servers, firewalls and customer data. Criminal activity is suspected. Maximum response time for the incident is 30 minutes.


Incident Detected
Incident electronically sent to Agency Point-of Contact (POC)
Agency Incident Response Procedures Activated
Documentation and afteraction report sent to BEA
Incident Electronically Sent To ISD On-Call Person
YES
ISD will contact Agency POC
Low Level Incident Detected
ISD will report the incident to the CISO the next business day
NO
ISD will contact Agency POC
Report Incident to EA & I&O Directors the next business day
3
Medium Level Incident Detected
YES
ISD will contact CISO
Notify I&O CIRT Team
no
Yes
Contact I&O CIRT Team to activate incident response procedures
NO
ISD will contact Agency POC
YES
High Level Incident Response
ISD Personnel will contact CISO
CISO will contact EA and I&O Directors
EA or I&O Director will contact CIO
CIO will contact Agency Dep Secretary for Admin or Agency Head
NO
2
CISO or ISD under the direction of the CISO will:
1

Legend

CIO - Chief Information Officer
CISO - Chief Information Security Officer
CIRT - Computer Incident Response Team
BEA - Bureau of Enterprise Architecture
FedCIRC - Federal Computer Incident Response Center
I&O - OA Infrastructure and Operations Bureau
ISD - Information Security Division of the EA Bureau
MS-ISAC - Multi-State Information and Sharing and Analysis Center
POC - Point of Contact
PSP - Pennsylvania State Police


1
Contact Office of General Counsel
Contact Appropriate Criminal Justice Authorities: PSP Capitol Police
Contact I&O CIRT Team to activate incident response procedures
Contact Human Resources
Contact Communications Office to interact with the news media
Federal guidelines may require contacting FedCIRC, MS-ISAC or other reporting agencies
2
Incident Has not been documented
Treat incident as a medium level threat until analysis indicates otherwise
3

Legend

CIO - Chief Information Officer
CISO - Chief Information Security Officer
CIRT - Computer Incident Response Team
BEA - Bureau of Enterprise Architecture
FedCIRC - Federal Computer Incident Response Center
I&O - OA Infrastructure and Operations Bureau
ISD - Information Security Division of the EA Bureau
MS-ISAC - Multi-State Information and Sharing and Analysis Center
POC - Point of Contact
PSP - Pennsylvania State Police

Point of Contact (POC). Each agency must supply to the Information Security Division of Enterprise Architecture a primary and secondary point of contact. The point of contact must not have administrator responsibilities. This will preclude any possibility of a POC being the object of the incident. It is preferable that the main contact is the agency chief security officer. The agency chief security officer will notify the privacy and policy officer of the incident as soon as possible. Several communication methods (email, cell phone, home phone) must be supplied so there is no single point of failure in contacting the individual(s).

Each agency must supply to the Information Security Division of Enterprise Architecture a primary and secondary point of contact. It is preferable that the main contact is the agency chief security officer. The agency chief security officer will follow their internal notification policy as soon as possible after being informed of an incident. Several communication methods (email, cell phone, home phone) must be supplied so there is no single point of failure in contacting the individual(s).

See Enclosure 4 for POC format template.

Documentation and After Action Reports. The affected agency Chief Security Officer will appoint a person(s) to be responsible for documenting the incident and its resolution. The agency will hold a "lessons learned" meeting to review how effective the incident handling process was and identify necessary improvements to existing security controls and practices. Documentation and the after action report will be forwarded to the Office of Administration Deputy Secretary for Information Technology within 15 business days of the incident. **See Enclosure 5 for incident response documentation templates.**

Point of Contact Information Template

Name: ____

Agency: ____

Bureau: ____

Title: ____

Work Phone: ____

Home Phone: ____

Mobile Phone: ____

Fax Number: ____

Pager: ____

Work Address: ____

Security Incident Detector’s Information

Detectors Name: ______________________________

Agency: ______________________________

Bureau: ______________________________

Title: ______________________________

Work Phone: ______________________________

Home Phone: ______________________________

Mobile Phone: ______________________________

Fax Number: ______________________________

Pager: ______________________________

Work Address: ______________________________

Date/Time Incident Detected: ______________________________

Location Incident Detected From: ______________________________

Incident Summary

Type of Incident Detected (i.e. DOS, Malware, Unauthorized Access): ______________________________

____

Incident Location

Site Address: ______________________________

Site POC Name: ______________________________

Title: ______________________________

Work Phone: ______________________________

Home Phone: ______________________________

Mobile Phone: ______________________________

Fax Number: ______________________________

Pager: ______________________________

Work Address: ______________________________

Describe the information system affected: ______________________________

____

Describe the physical security of the location of the affected information system: ______________________________

____

Incident Containment

Was the affected system removed from the network? ____ Yes ____ NO

If YES, date/time removed from network: ____

If NO, state the reason: ____

Backup of Affected Systems

Was a backup performed on the affected system: ____ YES ____ NO

If YES,

Name of Person who performed the backup: ____

Work Phone: ____

Date/Time Backup Started: ____

Date/Time Backup Completed: ____

Backup Tapes Sealed: ____ YES ____ NO

Backup Tapes Turned Over To: ____

Incident Eradication

Name of Person(s) performing forensics on system: ____

Work Phone: ____

Was the vulnerability identified? ___ YES ___ NO

Explain ____

____

Explain the procedure, in detail, used to fix the problem. ____

____

____

Did detection occur promptly or if not why not? ____

____

What additional tools could have helped the detection or eradication process? _____________________________

____

Was communication adequate or could it have been better? ____

____

What practical difficulties were encountered? ____

____

Estimated cost of the incident to the Agency. ____

Was any data irrecoverably lost, and if so the estimated value of the data? _____________________________

____

Was any hardware damaged? ____

____