

INSERT COMPANY NAME AND/OR LOGO

## System Security Plan (SSP) Appendixes

*Draft Version 1*

Date Revised: 8/23/2016

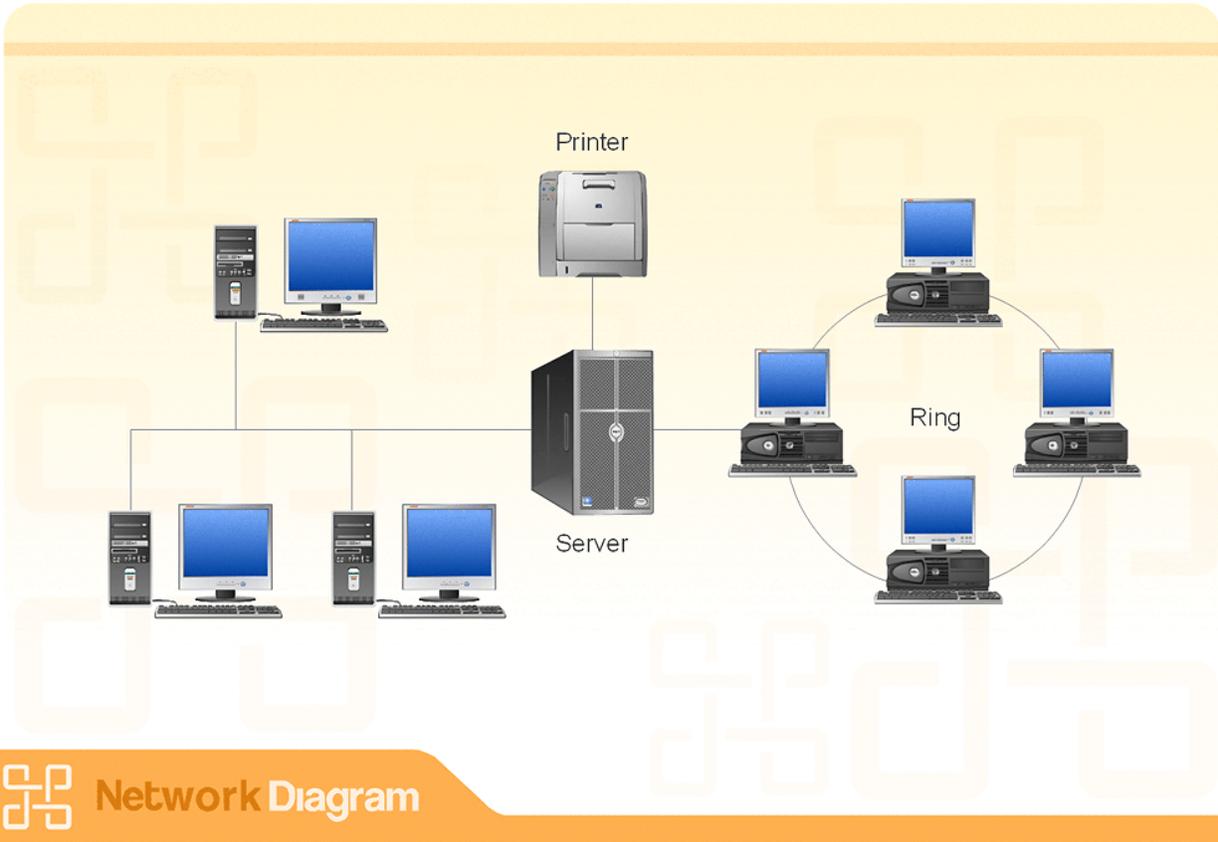
## CONTENTS

---

1	Appendix A: System/Network Diagram.....	3
2	Appendix B: Facility/System Layout .....	4
3	Appendix C: Hardware List .....	5
4	Appendix D: Software List .....	6
5	Appendix E: Record of Controlled Area (DSS Form 147) .....	7
6	Appendix F: IS Access Authorization and Briefing Form.....	7
7	Appendix G: Upgrade/Downgrade Procedure Record .....	8
8	Appendix H: IS Security Seal Log .....	9
9	Appendix I: Maintenance, Operating System & Security Software Change Log.....	10
10	Appendix J: Assured File Transfer Procedures.....	11
11	Appendix K: Contingency Plan Template.....	12
12	Appendix L: In Response Plan Template.....	19
13	Appendix M: Plan of Action & Milestones .....	23
14	Appendix N: Risk Assessment Report.....	24
15	Appendix O: Mobility System Plan .....	24
16	Appendix P: Risk Acknowledgement Letter.....	25
17	Appendix Q: Other Applicable Documentation or Standard Operating Procedures .....	26

# 1 APPENDIX A: SYSTEM/NETWORK DIAGRAM

**SAMPLE DIAGRAM** - Create a diagram for the information system (E.G. Data flows between, and is stored on, all workstations based on user groups.)



## **2 APPENDIX B: FACILITY/SYSTEM LAYOUT**

---

<Insert facility, floor plan, and system layout as appropriate>





## 5 APPENDIX E: RECORD OF CONTROLLED AREA (DSS FORM 147)

RECORD OF CONTROLLED AREA <small>(May also be used for recording approval of vaults and strong rooms)</small>			
1. TYPE: <input type="checkbox"/> Closed Vault <input type="checkbox"/> Spec. Container  Class: <input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> Modular	2. FACILITY NAME AND ADDRESS:	3. IDENTITY OF AREA, NUMBER AND LOCATION:  3a. Normal Hours of operations:	4. APPROVED DEGREE OF STORAGE:  4a. Type of Material Safeguarded:  4b. Open Storage: <input type="checkbox"/> Yes <input type="checkbox"/> No
5. NAME AND TITLES OF FACILITY PERSONNEL CONSULTED:		6. Date of inspection:	
CONSTRUCTION FEATURES			
7. WALLS: Do walls extend to true ceiling? <input type="checkbox"/> Yes <input type="checkbox"/> No	8. DOORS: How many? _____ Entry/Exit _____ Non-Entry/Exit _____ Description:		13. DOOR LOCKING DEVICES a. During working hours b. During non-working hours c. Non-entry doors
9. CEILINGS:  9a. If a false ceiling, the ceiling or space above is checked on a (weekly, monthly, biannual) basis or secured as follows:	10. FLOORS:  10a. If a raised floor, the space below or crawl ways are checked on a (weekly, monthly, biannual) basis or secured as follows:		14. SUPPLEMENTAL PROTECTION: a. Alarm System (1) Monitor: <input type="checkbox"/> Proprietary <input type="checkbox"/> Sub-contract (2) Type: <input type="checkbox"/> Central <input type="checkbox"/> Direct <input type="checkbox"/> Local (3) U.L. (CRZH) Certificate Checked <input type="checkbox"/> Yes <input type="checkbox"/> No b. Guards (1) <input type="checkbox"/> Proprietary <input type="checkbox"/> Contractor (2) Frequency of Rounds _____ (3) <input type="checkbox"/> Alarm Response Only c. Security-In-Depth (SID): <input type="checkbox"/> Yes <input type="checkbox"/> No
11. WINDOWS: How many? _____ Opaque _____ Non-Opaque _____ Description:	12. MISCELLANEOUS OPENINGS:		15. UNUSUAL FEATURES OF CONSTRUCTION:
SIGNATURE OF IS REPRESENTATIVE(S) APPROVING AREA:		FIELD OFFICE:	SIGNATURE OF FACILITY SUPERVISOR:

DSS Form 147, APR 00

<Insert approved DSS form 147(s) here>

## 6 APPENDIX F: IS ACCESS AUTHORIZATION AND BRIEFING FORM

Printed Name: \_\_\_\_\_

Phone: \_\_\_\_\_

### Acknowledgment of Briefing

7

[Insert Classification]

I understand that as an Information Systems (IS) user, it is my responsibility to comply with all security measures necessary to prevent any unauthorized disclosure, modification, or destruction of information. I have read or will read all portions of the System Security Plan (SSP) pertaining to my level of responsibilities and agree to the following:

1. Protect and safeguard information in accordance with the SSP.
2. Sign all logs, forms and receipts as required.
3. Obtain permission from the ISSM or designee prior to adding/removing/or modifying any system hardware or software.
4. Ensure all files and media are checked for viruses and malicious logic using a current virus detection tool prior to, or at the time of introduction to an IS.
5. Escort non-authorized personnel in such a manner as to prevent their access to data they are not entitled to view.
6. I will comply with the following password requirements:
  - a) I will select a password that is a minimum of 14 non-blank characters for non-privileged accounts and 15 characters in length for privileged accounts. The password I select will contain a string of characters that does not include the user's account name or full name; includes one or more characters from at least 3 of the following 4 classes: Uppercase, lowercase, numerical & special characters.
  - b) Protect system passwords commensurate with the level of information processed on the system and never disclose to any unauthorized persons.
  - c) If I have access to a Generic or Group account, I will first login with my personal user id prior to accessing the Generic/Group account.
7. Protect all media used on the system by properly classifying, labeling, controlling, transmitting and destroying it in accordance with security requirements and security classification guide.
8. Protect all data viewed on the screens and/or outputs produced at the level of system processing until it has been reviewed.
9. I understand I must be authorized in writing by the ISSM to perform a Trusted Download. If authorized, I will perform this in accordance with the Trusted Downloading Procedures.
10. Notify the ISSM or designee when I no longer have a need to access the system (i.e.: transfer, termination, leave of absence or for any period of extended non-use).
11. Use the system for performing assigned company duties, never personal business.
12. Comply with all software copyright laws and licensing agreements.
13. I understand that all of my activities on the IS are subject to monitoring and/or audit.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

*6.1.1.1.1.1.1.1 FOR SECURITY AND ADMINISTRATOR USE ONLY*

Employee Visitor / Company: \_\_\_\_\_ Visit request expires on \_\_\_\_\_

Clearance/ Special Briefings: \_\_\_\_\_ Verified By: \_\_\_\_\_

Account Name: \_\_\_\_\_ Date Added: \_\_\_\_\_

Type of Account: General  Privileged

Other Access/Privileges, or Comments: \_\_\_\_\_

## **7 APPENDIX G: UPGRADE/DOWNGRADE PROCEDURE RECORD**

### UPGRADE PROCEDURES

1. Clear area of unauthorized persons and verify classified processing sign is posted.
2. Obtain classified media from approved storage.
3. Inspect Security Seals.
4. Install classified drive(s).
5. Boot system.
6. Document upgrade action below.

### DOWNGRADE PROCEDURES

1. Verify classified material has been removed from printer(s).
2. Verify classified hard drive, CDs, and Floppy Disks are removed.
3. Shutdown, power down system for 30 seconds.
4. Document downgrade action below.




**9 APPENDIX I: MAINTENANCE, OPERATING SYSTEM & SECURITY SOFTWARE CHANGE LOG**

---



## **11 APPENDIX K: CONTINGENCY PLAN TEMPLATE**

---

The Contingency Plan Template is intended as a guideline; each Program will need to adjust the Plan to meet their specific requirements.

### **I. Introduction**

The <Program Name> <click here to enter System Name> Contingency Plan (CP), documents the strategies, personnel, procedures, and resources required to respond to any short or long term interruption to the system.

## II. Scope

This CP has been developed for <click here to enter System Name> which is classified as a <moderate-low-low> impact system for the three security objectives: confidentiality, integrity, and availability. The procedures in this CP have been developed for a moderate-low-low impact system and are designed to recover the <click here to enter System Name> within <Recovery Time Objective (RTO)> hours. The replacement or purchase of new equipment, short-term disruptions lasting less than <RTO> hours, or loss of data at the primary facility or at the user-desktop levels is outside the scope of this plan.

**Note:** Recovery Time Objective (RTO) defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and supported mission/business processes.

## III. Assumptions

*Instruction: A list of default assumptions are listed in the section that follows. The assumptions should be edited, revised, and added to so that they accurately characterize the information system described in this plan.*

- a. The Uninterruptable Power Supply (UPS) will keep the system up and running for <total number of seconds/minutes>.
- b. The generators will initiate after <total number of seconds/minutes> from time of a power failure.
- c. Current backups of the application software and data are intact and available at the offsite storage facility in <City, State>.
- d. The <Information System Name> is inoperable if it cannot be recovered within <RTO hours>.
- e. Key personnel have been identified and are trained annually in their roles.
- f. Key personnel are available to activate the CP.

## IV. Roles and Responsibilities

The <click here to enter System Name> roles and responsibilities for various task assignments and deliverables throughout the contingency planning process are depicted in the table below.

Roles	Responsibilities
INFORMATION SYSTEM OWNER/PROGRAM MANAGER (ISO/PM) – Disruption Occurs	The responsibilities of the ISO/PM when a disruption occurs are listed but not limited to the following: <Click here to enter responsibilities> <Click here to enter responsibilities> <Click here to enter responsibilities>
SYSTEM ADMINISTRATOR (SA)	The responsibilities of the SA are listed but not limited to the following: <Click here to enter responsibilities> <Click here to enter responsibilities> <Click here to enter responsibilities>
PROGRAM SECURITY OFFICER (PSO)	The responsibilities of the PSO are listed but not limited to the following: <Click here to enter responsibilities> <Click here to enter responsibilities> <Click here to enter responsibilities>
INFORMATION SYSTEM SECURITY MANAGER/INFORMATION SYSTEM SECURITY OFFICER (ISSM/ISSO)	The responsibilities of the ISSM/ISSO are listed but not limited to the following: <Click here to enter responsibilities> <Click here to enter responsibilities> <Click here to enter responsibilities>

## V. System Description and Architecture

(It is necessary to include a general description of the system covered in the CP. The description should include the IT system architecture, location(s), and any other important technical considerations.)  
 Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.

## VI. Contingency Plan Phases

This plan has been developed to recover and reconstitute the <Information System Name> using a three-phased approach. The approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. The three system recovery phases consist of activation and notification, recovery, and reconstitution.

### 1. Activation and Notification Phase

Activation of the CP occurs after a disruption, outage, or disaster that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss.

Once the CP is activated, the information system stakeholders are notified of a possible long-term outage, and a thorough outage assessment is performed for the information system. Information from the outage assessment is analyzed and may be used to modify recovery procedures specific to the cause of the outage.

### 2. Recovery Phase

The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level such that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system stakeholders.

### 3. Reconstitution

The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating data and operational functionality followed by deactivation of the plan.

During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

## VII. Data Backup Readiness Information

The hardware and software components used to create the <Information System Name> backups are noted in Table 3-1.

*Table 1. Backup System Components*

System/Component	Description
Software Used	
Hardware Used	
Date of Last Backup	
Backup Type (Full, Differential, Incremental)	

## VIII. Alternate Site/Backup Storage Information

Alternate facilities have been established for backup storage and/or restoration of the <Information System Name> as noted in Table 3-2. Current backups of the system configuration, software and data are intact and available at the alternate storage facility.

Table 2. Primary and Alternate Site Locations

Designation	Site Name	Site Type (Hot, Cold, Warm, Mirrored)	Address
Primary Site			
Alternate Site			
Alternate Site			

## IX. Activation and Notification

The activation and notification phase defines initial actions taken once a disruption has been detected or appears to be imminent. The Recovery Time Objective (RTO) defines the maximum amount of time that the information system can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the maximum tolerable downtime. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the maximum tolerable downtime. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the CP. At the completion of the Activation and Notification Phase, key CP staff will be prepared to perform recovery measures to restore system functions.

### Activation Criteria

The CP may be activated if one or more of the following criteria are met:

1. The type of outage indicates <Information System Name> will be down for more than <RTO hours>;
2. The facility housing <Information System Name> is damaged and may not be available within <RTO hours>;
3. Other criteria, as appropriate.

## X. Recovery

The recovery phase provides formal recovery operations that begin after the CP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate individuals have been mobilized. Recovery phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the recovery phase, <Information System Name> will be functional and capable of performing essential functions.

### 1. Sequence of Recovery Operations

*Instruction: Modify the following list as appropriate for the system recovery strategy.*

1. Identify recovery location (if not at original location)
2. Identify required resources to perform recovery procedures
3. Retrieve backup and system installation media
4. Recover hardware and operating system (if required)
5. Recover system from backup and system installation media
  - g. Implement transaction recovery for systems that are transaction-based.

### 2. Recovery Procedures

*Instruction: Provide general procedures for the recovery of the system from backup media. Specific keystroke-level procedures may be provided in an appendix. If specific procedures are provided in an appendix, a reference to that appendix should be included in this section. Teams or persons responsible for each procedure should be identified.*

The following procedures are provided for recovery of <Information System Name> at the original or established alternate location. Recovery procedures should be executed in the sequence presented to maintain an efficient recovery effort. <Describe recovery procedures.>

## XI. Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant

change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan. Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

## 1. Data Validation Testing

*Instruction: Describe procedures for testing and validation of data to ensure that data is correct and up to date as of the last available backup. Teams or persons responsible for each procedure should be identified. An example of a validation data test for a moderate-impact system would be to compare a database audit log to the recovered database to make sure all transactions were properly updated. Detailed data test procedures may be provided in Appendix E, System Validation Test Plan.*

## 2. Functional Validation Testing

*Instruction: Describe procedures for testing and validation functional and operational aspects of the system.*

Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

## 3. Recovery Declaration

Upon successfully completing testing and validation, the <role name> will formally declare recovery efforts complete, and that <Information System Name> is in normal operations. <Information System Name> users and technical POCs will be notified of the declaration by the <role name>. The recovery declaration statement notifies the stakeholders and management that the <Information System Name> has returned to normal operations.

# XII. Post Reconstitution

## 1. Cleanup

*Instruction: Describe cleanup procedures and tasks including cleanup roles and responsibilities. Insert cleanup responsibilities in Table 7-1. Add additional rows as needed.*

manuals or other documentation to their original locations, and readying the system for a possible future contingency event.

*Table 1. Cleanup Roles and Responsibilities*

Role	Cleanup Responsibilities

## 2. Backup Procedures

*Instruction: Provide procedures for returning retrieved backup or installation media to its offsite data storage location. This may include proper logging and packaging of backup and installation media, preparing for transportation, and validating that media is securely stored at the offsite location.*

*Instruction: Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time frame, ideally at the next scheduled backup period.*

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are:  
<Enter procedure>

### 3. After Action Reporting

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort. Information on lessons learned should be included in the annual update to the CP. It is the responsibility of each CP team or person to document their actions during the recovery event.

## XIII. Contingency Plan Testing

Contingency Plan operational tests of the <Information System Name> are performed **at least annually**. A Contingency Plan Test Report is documented after each annual test.

*Instruction: Please describe the procedures for the annual contingency plan testing. Include a description of the required test environment. Operational tests typically include the following:*

- a. Restore files from backup tapes
- b. Verify that backup tapes are stored at designated off-site locations
- c. Determine whether data stored on backup tapes is valid and retrievable
- d. Perform failover testing
- e. Test the UPS to ensure that it operates correctly in the event of a power disruption;
- f. Test the offsite backup vendor's delivery response timeliness of media during normal daytime hours and during nighttime hours
- g. Test to ensure that offsite storage vendor only supplies backup tapes to authorized individuals
- h. Test the generators to ensure that they turn on automatically
- i. Perform tabletop exercises to test various possible contingency situations
- j. Perform call tree exercises to ensure that employees can be reached in a timely manner.

*Whatever methods you use to test your plan, please describe those tests in this section.*

# Contingency Plan Testing Report Template

*Instruction: This section should include a summary of the last Contingency Plan Test.*

Test Information	Description
Name of Test	
System Name	
Date of Test	
Team Test Lead and Point of Contact	
Location Where Conducted	
Participants	
Components	
Assumptions	
Objectives	Assess effectiveness of system recovery at alternate site Assess effectiveness of coordination among recovery teams Assess systems functionality using alternate equipment Assess performance of alternate equipment Assess effectiveness of procedures Assess effectiveness of notification procedures
Methodology	
Activities and Results (Action, Expected Results, Actual Results)	
Post Test Action Items	
Lessons Learned and Analysis of Test	
Recommended Changes to Contingency Plan Based on Test Outcomes	

## 12 APPENDIX L: INCIDENT RESPONSE PLAN TEMPLATE

The Incident Response Plan Template is intended as a guideline; each Program will need to adjust the Plan to meet their specific requirements.

### I. Introduction

The <Program Name> <click here to enter System Name> Incident Response Plan (IRP), documents the strategies, personnel, procedures, and resources required to respond to any incident affecting the system.

### II. Scope

This IRP has been developed for <click here to enter System Name> which is classified as a <moderate-low-low> impact system for the three security objectives: confidentiality, integrity, and availability.

### III. Roles and Responsibilities

The <click here to enter System Name> roles and responsibilities for various task assignments and deliverables throughout the incident response process are depicted in the table below.

Roles	Responsibilities
INFORMATION SYSTEM OWNER/PROGRAM MANAGER (ISO/PM) – Incident Occurs	The responsibilities of the ISO/PM when an incident occurs are listed but not limited to the following: <Click here to enter responsibilities> <Click here to enter responsibilities> <Click here to enter responsibilities>
SYSTEM ADMINISTRATOR (SA)	The responsibilities of the SA are listed but not limited to the following: <Click here to enter responsibilities> <Click here to enter responsibilities> <Click here to enter responsibilities>
PROGRAM SECURITY OFFICER (PSO)	The responsibilities of the PSO are listed but not limited to the following: <Click here to enter responsibilities> <Click here to enter responsibilities> <Click here to enter responsibilities>
INFORMATION SYSTEM SECURITY MANAGER/INFORMATION SYSTEM SECURITY OFFICER (ISSM/ISSO)	The responsibilities of the ISSM/ISSO are listed but not limited to the following: <Click here to enter responsibilities> <Click here to enter responsibilities> <Click here to enter responsibilities>

### IV. Definitions

#### 1. Event

An event is an occurrence not yet assessed that may affect the performance of an information system and/or network. Examples of events include an unplanned system reboot, a system crash, and packet flooding within a network. Events sometimes provide indication that an incident is occurring or has occurred.

#### 2. Incident

An incident is an assessed occurrence having potential or actual adverse effects on the information system. A security incident is an incident or series of incidents that violate the security policy. Security incidents include penetration of computer systems, spillages, exploitation of technical or administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code.

## V. Types of Incidents

The term "incident" encompasses the following general categories of adverse events:

**Data Destruction or Corruption.** The loss of data integrity can take many forms including changing permissions on files so that they are writable by non-privileged users, deleting data files and or programs, changing audit files to cover-up an intrusion, changing configuration files that determine how and what data is stored and ingesting information from other sources that may be corrupt.

**Data Compromise and Data Spills.** Data compromise is the exposure of information to a person not authorized to access that information either through clearance level or formal authorization. This could happen when a person accesses a system he is not authorized to access or through a data spill. Data spill is the release of information to another system or person not authorized to access that information, even though the person is authorized to access the system on which the data was released. This can occur through the loss of control, improper storage, improper classification, or improper escorting of media, computer equipment (with memory), and computer generated output.

**Malicious Code.** Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem.

**Virus Attack.** A virus is a variation of a Trojan horse. It is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data). Often self-replicating, the malicious program segment may stand-alone or may attach itself to an application program or other executable system component in an attempt to leave no obvious signs of its presence.

**Worm Attack.** A computer worm is an unwanted, self-replicating autonomous process (or set of processes) that penetrates computers using automated hacking techniques. A worm spreads using communication channels between hosts. It is an independent program that replicates from machine to machine across network connections often clogging networks and computer systems.

**Trojan Horse Attack.** A Trojan horse is a useful and innocent program containing additional hidden code that allows unauthorized computer network exploitation (CNE), falsification, or destruction of data.

**System Contamination.** Contamination is defined as inappropriate introduction of data into a system not approved for the subject data (i.e., data of a higher classification or of an unauthorized formal category).

**Privileged User Misuse.** Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains.

**Security Support Structure Configuration Modification.** Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled since they are essential to maintaining the security policies of the system. Unauthorized modifications to these configurations can increase the risk to the system.

**Note: These categories of incidents are not necessarily mutually exclusive.**

## VI. Incident Response

<Program Name> shall follow the incident response and reporting procedures articulated in AR 380-381, Section 5.9. Upon learning of an incident or a data spillage, the PD/PM and PSO/PSM will take immediate steps aimed to minimize further damage and/or regain custody of the information, material or mitigate damage to program security. Within 24 hours of notification of the incident, the PD/PM will notify the DCS, G-2, the TMO (Security,) and the normal SAP reporting chain of command (to include the covering CI agent). The PD/PM will provide an updated report to the DCS, G-2 and ASPD not later than 72 hours after the incident. The PD/PM will provide the DCS, G-2 and the TMO a final report in every case, however the due date is case specific (reasonable time period to be decided by the DCS, G-2 and the TMO).

In those cases involving an information system, the PM/PD shall notify the G-2 and the CIO/G-6 SAP/SA Special Programs Office/AO to determine the appropriate actions required to mitigate the incident. At this time the AO shall make a determination whether the IS can be allowed to continue processing or must be disconnected until further resolution.

Incident response will follow the following six steps:

- h. Preparation – one of the most important facilities to a response plan is to know how to use it once it is in place. Knowing how to respond to an incident BEFORE it occurs can save valuable time and effort in the long run.
- i. Identification – identify whether or not an incident has occurred. If one has occurred, the response team can take the appropriate actions.
- j. Containment – involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment.

- k. Eradication – removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators, or dismissing employees.
- l. Recovery – restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that the system is back to its normal condition.
- m. Follow-up – some incidents require considerable time and effort. It is little wonder, then, that once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law. This includes changing any company policies that may need to be narrowed down or be changed altogether.

## **VII. Incident Response Training**

All Program personnel will receive incident response training at least annually and a record of the training will be maintained. This training can be integrated into the overall Program-specific annual security awareness training.

# Incident Response Worksheet

SECURITY INCIDENT REPORT			
<b>Report Classification:</b>			
<b>Report No.:</b>		<b>Report Organization:</b>	
<b>Report Date:</b>		<b>Report Type</b> (initial, final, status):	
<b>Report Generated By:</b>		Date:	Time:
Title:	Telephone:	E-mail:	
Signature:			
<b>SECTION 1 – POC Information</b>			
Incident Reported By:		Date:	Time:
Location:	Telephone:	E-mail:	
Signature:			
PSO/ISSM Notified (Name):		Date:	Time:
Location:	Telephone:	E-mail:	
Signature:			
ASPD Notified (Name):		Date:	Time:
Location:	Telephone:	E-mail:	
Method of Notification:			
G-2 Notified (Name):			
Date:	Time:		
Office:	Telephone:	E-mail:	
Method of Notification:			
<b>SECTION 2 – Incident Information</b>			
Date of Incident:		Time of Incident:	Ongoing?
Incident Facility Name:		Incident Facility Location:	
Affected Computer Systems (Hardware and/or Software):			
Classification of Affected Computer Systems:			
Physical Location of Affected Systems:			
Connections of Affected Systems to Other Systems:			
Type of Incident (Data Destruction/Corruption, Data Spill, Malicious Code, Privileged User Misuse, Security Support Structure Configuration Modification, System Contamination, System Destruction/Corruption/Disabling, Unauthorized User Access, other – please identify):			
Suspected Method of Intrusion/Attack:			
Suspected Perpetrator(s) or Possible Motivation(s):			
Apparent Source (e.g., IP address) of Intrusion/Attack:			
Apparent Target/Goal of Intrusion/Attack:			
Mission Impact:		Success/Failure of Intrusion/Attack:	
Attach technical details of incident thus far. Include as much as possible about the Detection and Identification, Containment, Eradication, and Recovery – steps taken (with date/time stamps), persons involved, files saved for analysis, etc.			

## **13 APPENDIX M: PLAN OF ACTION & MILESTONES**

---

<Insert Unclassified POA&M or location of document>

## **14 APPENDIX N: RISK ASSESSMENT REPORT**

---

<Insert Unclassified RAR or location of document>

## **15 APPENDIX O: MOBILITY SYSTEM PLAN**

---

<If Applicable, Insert mobility plan>

## **16 APPENDIX P: RISK ACKNOWLEDGEMENT LETTER**

---

<If Applicable, insert RAL>

## **17 APPENDIX Q: OTHER APPLICABLE DOCUMENTATION OR STANDARD OPERATING PROCEDURES**

---

<Add additional Unclassified documentation or SOPs as applicable to further describe implemented controls in SSP such as; Continuous Monitoring strategy, Configuration Management (CM), Memorandum of Agreements (MOU)/Interconnected System Agreements (ISA), Protected Distribution System (PDS) approvals etc.>