APPENDIX F: INCIDENT RESPONSE PLAN

Introduction

The TEMPLATECLIENT Incident Response Plan (IRP), documents the strategies, personnel, procedures, and resources required to respond to any incident affecting the system.

Scope

This IRP has been developed for TEMPLATECLIENT., which is classified as a moderate impact system for the three security objectives: confidentiality, integrity, and availability.

Roles and Responsibilities

The TEMPLATECLIENT roles and responsibilities for various task assignments and deliverables throughout the incident response process are depicted in the table below.

Table 1: Roles and Responsibilities

Roles	Responsibilities
Information System Owner	Annual review of SSP, annual test of IRP. Ensure that Security Manager and TEMPLATECLIENT systems administrators are properly trained, and have resources required to maintain an incident response capability.
Security Manager	Oversee and prioritize actions during the detection, analysis, and containment of an incident.
IT Department	Work directly with Security Manager and Information Systems Owner throughout the six steps of Incident Response.

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.

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 be 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.

Incident Response

TEMPLATECLIENT shall follow the incident response and reporting procedures specified in the SSP. Upon learning of an incident or a data spillage, the Security Manager will take immediate steps intended to minimize further damage and/or regain custody of the information, material or mitigate damage to program security.

Incident response will follow the following six steps:

1. 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.
2. Identification – identify whether or not an incident has occurred. If one has occurred, the response team can take the appropriate actions.
3. 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.
4. Eradication – removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators, or dismissing employees.
5. 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.
6. 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.

Incident Response Training

All TEMPLATECLIENT employees who have a role in Incident Response 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.

Table 2: Incident Response Worksheet

SECURITY INCIDENT REPORT SECTION 1 – POC Information			
Report Classification:			
Report No.:		Report Organization:	
Report Date:		Report Type (initial, final, status):	
Report Generated By:		Date:	Time:
Title:	Telephone:	E-mail:	
Signature:			
SECTION 1 – POC Information			
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:			
SECTION 2 – Incident Information			
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 Perpetrators or Possible Motivations:			
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.			