INCIDENT RESPONSE PLAN

INTRODUCTION

In accordance with industry best practices and to comply with applicable compliance regulations, the provider has implemented a range of procedures, policies, and guidelines to protect the confidentiality, integrity, and availability (CIA) of critical client data and computing resources.

As new technologies and requirements emerge, this document may need to be updated and should be reviewed at least annually. This function will be performed by members of the security team under the direction of the Chief Technology Security Officer.

OVERVIEW

Security incidents can vary widely in severity, and not all incidents will require the same level of attention. It is important to be prepared and to understand that different phases exist in responding to an incident, as well as the goals and objectives of each phase.

The phases of a security incident response plan at the provider are as follows:

PREPARE

- Ensure the incident-handling team includes technical experts, human resources, and customer-facing personnel.
- Staff should be trained at the appropriate level.
- Contact information is included as an appendix to this document.
- Backups must be taken and tested.

IDENTIFY

Awareness that a security incident has occurred may originate from technical personnel, end users, or even clients.

An incident should be declared when security personnel detect or suspect an adverse risk to the company. Once identified, the team must assemble and implement the plan.

CONTAIN

Containment procedures will vary depending on the nature of the incident and the direction of the business owner. A compromised machine may not present valid data, so containment should consider the following:

- Obtain and analyze as much system information as possible, including key files and potentially a backup of the compromised device for later forensic analysis.
- Powering off a machine may result in data loss. If possible, avoid powering it off.
- Disconnecting the machine from the network may help containment and forensic activity. (Connecting the computer to a separate network with a network analyzer may assist in evaluating network activity.)

If one machine has been exploited, others may be vulnerable. Large-scale containment actions may include:

- Downloading security patches from vendors
- Updating antivirus signatures
- Closing firewall ports
- Disabling compromised accounts
- Running vulnerability analyzers to identify other vulnerable hosts
- Changing passwords as appropriate

ERADICATE

Eradication procedures depend on the nature of the incident and the direction of the business owner. Key considerations:

- Boot CDs should be used to access and analyze compromised machines. (Rootkits installed on compromised machines may affect basic system utilities and discourage use of potentially compromised components.)
- If an operating system has been compromised, the machine should be rebuilt using hardened images for the appropriate platforms.
- Backups should be tested to ensure they are usable for restoring the system or responding to a new incident.

RECOVERY

Specific recovery actions depend on the type of incident and the direction of the business owner. Key considerations include:

- Retesting the system thoroughly with a variety of end users

- Considering timing and readiness for a return to production
- Discussing customer notification and associated concerns
- Discussing media-handling considerations
- Continuing to monitor for security incidents

REVIEW

A final report should be written describing the incident and how it was handled. This report should include:

- Recommendations for addressing future incidents
- Adjustments to this document as needed