Information Security Incident Response Plan

1.0 PURPOSE

The purpose of this Information Security Incident Response Plan is to establish a process for information security incident response, and to empower the incident response team (IRT) to ensure computer security incidents are reported properly and addressed with the appropriate response for the severity of the incident.

2.0 SCOPE AND INTRODUCTION

The scope of this plan includes all the organization's information systems. All employees, contractors, and temporary workers must follow the requirements set in this policy when responding to an information security incident.

Preparation for incident response has four components:

- Preparation for an incident response: Includes training on how to report incidents, and the contact information and roles of the members of the incident response team (IRT).
- Response to an incident: The actual response steps to use in any potential incident. The response has seven phases:
    - Incident detection
    - Evidence gathering
    - Analysis and determination of severity
    - Incident prioritization
    - Incident tracking
    - Containment
    - Response and recovery
- Post-incident activity: lessons learned and rules for retention of forensic data gathered during the response
- Incident response testing: Periodic testing and improvement of this plan

3.0 INCIDENT RESPONSE PROCEDURES

3.1 Preparation

3.1.1 Incident Reporting

The first step in incident response planning is educating users to detect and respond to incidents that threaten the security of the organization's systems. Any user who is aware of an event that might potentially be a security incident should immediately report that information to the IT department (Optimal). This will be communicated through security awareness training and other methods. The Incident Response Team (IRT) must be aware of their roles and responsibilities and should review this plan document annually.

3.1.2 Definition of Security Incident

A security incident is any incident that materially compromises the confidentiality, reliability or availability of key organization data or system. A potential security incident is any event that has the potential to have been an actual security incident before such time as a determination has been made as to whether an actual compromise occurred.

Breaches are security incidents in which it has been verified that confidentiality, integrity, or availability was materially affected by a malicious third party or it is reasonable to assume such effects.

This means that as a matter of organization policy, such a breach should initially be assumed to have occurred whenever there is unauthorized access to any premises or data, when computing or mobile devices are lost or stolen, or when any other type of security incident occurs. Similarly, all personnel must adopt the stance "if in doubt, report" so that any possible security weakness is properly raised and addressed, to eliminate the risk of any breach in the first place. It follows that a breach of any kind and severity should be reported – from suspected ransomware attack to emails being sent to the wrong recipient.

3.1.3 Incident Response Team

Informing the appropriate personnel is of extreme importance when responding to security incidents. A list of contacts is provided below. At a minimum, an incident response team (IRT) must include key officers of the organization and at least one member of the technology team. Incidents that are significant enough to cause an outage will be escalated to the organization's president. The IRT must be aware of their roles and responsibilities.

Name	Title	Phone	Email	Primary / Alternate	Role
Cynthia Arcuri	Chief Financial Officer	(484) 888-1947	CArcuri@tscalliance.org	Primary	Primary liaison between TSC Alliance and Optimal Networks
Rachel Wojnilower	Executive Assistant	(513) 238-6328	RWojnilower@tscalliance.org	Alternate	Alternate liaison between TSC Alliance and Optimal Networks
Frank Schipani	CIO Consultant	(240) 499-7974	fschipani@optimalnetworks.com	Primary	Primary contact for IT security issues
Jeremy Ziaee	Network Engineer	(240) 499-7900	jziaee@optimalnetworks.com	Primary	Primary contact for IT security issues

Optimal Networks Support Center	IT Department	(240) 499-7950	supportcenter@optimalnetworks.com	Alternate	Contact for general IT questions and alternate for IT security issues

3.1.4 Incident Communication

Control of information during a security incident or investigation of a possible incident is very important. Providing incorrect information or communicating using channels that are not secure can have undesirable side effects. The IRT is responsible for communication details of the incident to management. The IRT will also send incident response updates to personnel as appropriate. No one can comment or discuss a security incident with an individual who is not part of the organization, the organization's technology provider, or is designated as responsible the IRT. Email will be used as the preferred communication method for the IRT, unless there is suspicion that it has been compromised or is not accessible due to a loss of availability. If email has been compromised, Cynthia Arcuri and Rachel Wojnilower can be contacted via Slack or cell phone (call or text). Optimal can be contacted via their SupportCenter.

Cynthia Arcuri's Cell Phone – 484-888-1947

Rachel Wojnilower's Cell Phone – 513-238-6328

Optimal Network's SupportCenter – 240-499-7950

3.2 Response

3.2.1 Detection

This phase outlines the process the organization follows to detect a security incident.

If a potential security event has been observed, the employee must notify the IRT immediately. Notification of an incident can come from many various sources: users, automated monitoring tools, system logs, and anti-virus software.

A security incident is an observable occurrence in a network or system (e.g., known or suspected penetrations of IT resources, probes, infections, log reviews), or any occurrence that potentially could threaten organization data confidentiality, integrity, or availability. The table below identifies the most common security incidents that threaten data at the organization.

Incident Type	**Incident Definition**
System Compromise or Intrusion	All unintentional or intentional instances of system compromise or intrusion by unauthorized persons must be reported, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.
Malicious Code	All instances of successful infection or persistent attempts at infection by malicious code, such as viruses, malware, Trojan horses, or worms, must be reported.

Loss, Theft, or Missing	All instances of the loss or theft of laptop computers or other data-containing devices; and all instances of the loss or theft of IT resources, including media that contains sensitive information or PII.
Denial of Service	Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or one or more portions of a network must be reported. Critical services are determined through Business Impact Analyses in the Contingency Planning process.
Unauthorized Use	Any activity that adversely affects an information system's normal baseline performance and/or is not recognized. Unauthorized use includes, but is not limited to, port scanning that excessively degrades performance; IP (Internet protocol) spoofing; network reconnaissance; monitoring; hacking into organization systems; running traffic-generating applications that generate unnecessary network broadcast storms or drive large amounts of traffic to organization computers; or using illegal (or misusing copyrighted) software images, applications, data, and music. Unauthorized use can involve using organization systems to break the law.
Information Compromise	Any unauthorized disclosure of information that is released from control to entities that do not require the information that may occur due to inadequate clearing, purging, or destruction of media and related equipment or transmitting information to an unauthorized entity.
Web Site Defacement	All instances of a defaced organization web site must be reported.

Once notification occurs, the information should be passed on to the IRT as soon as possible. The IRT, with the assistance of third parties as needed, will use the Incident Response Action Form attached to this document (section 6.0) to determine if a security incident has occurred.

Optimal Networks will be responsible for the following procedures once notified of a possible incident:

- Evidence gathering
- Analysis and determination of severity
- Incident prioritization
- Incident tracking and documentation
- Containment
- Response and recovery

3.3 Post Incident Activity

3.3.1 Lessons Learned

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis must be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) must meet and discuss actions that were taken, and the lessons learned. All existing procedures should be

evaluated and, if necessary, modified. All online copies of infected files, malicious code, etc., must be removed from affected system(s). If applicable, a written incident report and set of recommendations should be presented to organization management.

3.3.2 Retention

Any devices or forensic images used during the incident investigation must be kept for a year after the incident occurs. These items may be used as evidence if law enforcement becomes involved and the case goes to court. Once the devices or forensic images are no longer needed, they must be destroyed.

3.4 Plan Testing

This incident response plan will be tested annually. This test should consist of tabletop scenarios designed to test the organization's incident response capabilities. These tests must be documented as if they were real incidents. Lessons learned from these tests provide guidance on improvements to the IRP and user training as needed.

4.0 REVISION HISTORY

Date	Revision #	Description of Change
2022-03-21	0.9	Initial creation
2022-09-01	0.91	Modifications to draft
2022-09-07	1.0	Finalized

5.0 SIGNOFF

This policy is approved by the policy owner, the Chief Financial Officer.

Printed name: Cynthia Arcuri

Signature: Cynthia Arcuri

Date: 11/14/22