Incident Response Policy

Revised: 7/17/18

Revision History

Version	Date	Author	Summary of Changes
1.0	07/17/2018	Armand Brunelle	Original Document

Approvals

Table of Contents

1.0 Incident Handling Policy

Control Number:

Control Objective:

Item Name:

Task:

1.1 Overview

Gabriel Software is dependent on data and network resources. Proper detection and response to incidents that may impact the integrity, confidentiality or availability of these resources is critical to the operation of the company. Such incidents include, but are not limited to: virus outbreaks, physical or remote security breaches, denial-of service attacks, and other exploited vulnerabilities.

The following standards were developed by Gabriel Software to prepare those employed by or affiliated with the company to properly detect and respond to incidents of any kind. Individuals are encouraged to implement any additional plans they deem necessary. These recommendations should not be used to reduce the level of preparedness that may already exist.

These minimum standards apply to all Gabriel Software departments and affiliates, as well as contractors and vendors handling Gabriel Software's systems or data. They represent the recommended minimum planning and cooperative efforts necessary to ensure the best incident detection and response possible.

1.2 Security Incident Detection

Gabriel Software users and administrators should be alert for symptoms that indicate and intrusion into their systems. The following points are helpful in detecting intrusions:

Be suspicious of unusual activity – unusual computer or network activity can be an indicator of a virus, attack, or intrusion. Activities and symptoms to look for include:

- Excessive virus warnings or personal firewall pop-up messages
- Unexpected system reboots and/or sudden degradation of system performance
- Unauthorized new user accounts or altered passwords
- New directories or files, often with unusual names such as "…" or " .."
- Modification or defacement of web sites
- New open network ports on a system
- Unexpectedly full disk drives

Listen to complaints received from others – comments or emails claiming suspicious activity from a computer may indicate the machine is infected or has been compromised and may actively be attacking other computers.

Be aware of the physical environment – access to secure areas at Gabriel Software is restricted, and situations to be aware of include:

- Unauthorized personnel in secure areas
- Unknown users at a computer
- Missing or moved equipment

- Open or unlocked doors that are normally secured

Gabriel Software regularly reviews server logs of Office 365 and the Azure Portal logs. These files are invaluable in detecting and tracking attempted intrusions and other suspicious activity. To maximize the value of logs, the Gabriel Software Systems Administrator:

- Ensures that a very high level of logging is enabled
- Checks logs regularly for suspicious activities and entries
- Monitors email alerts for suspicious activities
- Looks for missing time spans in logs
- Checks for repeated login failures or account lockouts
- Investigates unexpected system reboots
- Scans corporate antivirus logs for alerts and threat warnings

1.3 Incident Response

All Gabriel Software system users should immediately report suspicious activity via the Freshdesk Help Desk online at https://gabrielsoft.freshdesk.com . Administrators will refer to Gabriel Software's Incident Response Guidelines for technical assistance in investigating the incident.

This policy is applicable to any incident that occurs at Gabriel Software, including but not limited to security incidents, physical injury, theft, property damage, denial of service, threats, harassment and/or other criminal offenses involving individual user accounts, forgery and/or misrepresentation.

1.4 Definitions

Term	Definition
Incident	Any adverse event which compromises some aspect of Gabriel Software computer or network functionality/security, or business operations.
Vulnerability	A characteristic piece of technology which can be exploited to perpetrate a security incident.

2.0 Incident Response Guidelines

2.1 Overview

Gabriel Software computer users must be prepared to respond properly when a security incident occurs. Gabriel Software takes a proactive approach to incident handling. A solid plan of attack for different types of security incidents is crucial to the continuance and/or restoration of normal operations at Gabriel Software.

2.2 Purpose

The purpose of this document is to provide security personnel and administrators with guidelines for incident handling at Gabriel Software.

2.3 Scope

These minimum standards apply to all Gabriel Software departments and affiliates, including contractors and vendors handling Gabriel Software systems or data.

2.4 Guidelines

Responses to specific incidents may include:

2.4.1 Incident Evaluation and response

- Check all systems for new or modified accounts
- Review log files for abnormal entries or missing time spans
- Look for modifications made to system software and/or configuration files
- Scan system for new binaries (including user directories)
- Check other local systems and related remote systems
- Change system password(s)
- Clean and/or reformat the system as appropriate

2.4.2 Incident Reporting

- Fill out a help desk ticket via our online system at https://gabrielsoft.freshdesk.com
- If you are unable to access the help desk and/or after logging the incident in the help desk system, please follow up with a telephone call to the Gabriel Systems Administrator or your immediate manager to discuss the nature of the incident