Imprimis, Inc.

IT/Cybersecurity Incident Response Plan

Imprimis, Inc.
9-26-2016

Contents

1.0.0 Mission Statement

To maintain and utilize a robust incident-handling capability for organizational information and operational systems. This capability shall include preparation, detection, analysis, containment, recovery, and user response activities. The incident response (IR) capability shall be periodically reviewed and tested and updated based on these reviews and tests.

2.0.0 Introduction

This Incident Response Plan (IRP) is a reference for employees of Imprimis, Inc. and is intended provide a robust, efficient, and consistent process for incident response.

If an employee has a questions or concerns regarding this IRP, or his or her role in it, the employee is responsible for contacting his or her supervisor, manager, or Human Resource Representative for clarification.

3.0.0 Scope

This policy applies to all Imprimis, Inc. employees, contractors, vendors and agents with a company-owned or personally-owned computer, workstation, mobile, or other electronic device used to connect to any Imprimis, Inc. network or information system (IS).

4.0.0 Incident Definition

An incident is defined as an event which is not part of the standard operation of service and which causes or may cause disruption to or a reduction in the quality of services and user productivity.

5.0.0 Incident Response Team

The primary cyber incident response team (CIRT) will consist of the Information Technology Authority (ITA), IT Manager (ITM), IT Department, and the Security Officer. However, all personnel have a role in detecting potential incidents and in implementing certain response actions.

Role	Person(s) Appointed
CM – Corporate Management	CEO/President & Department VP's
SO – Security Officer	Facility Security Officer, Information System Security Manager, etc.
ITA – Information Technology Authority	CIO, IT Director, or Appointed Individual
ITM – Information Technology Manager	ITD Manager
ITD – Information Technology Department	IT Personnel
DM – Department Manager	Program Manager, HR Manager, Line Manager, etc.
User	Any user of any company IS

6.0.0 System Configurations for Incident Response

In order to have an effective IR process, it is essential that system tools be configured to provide sufficient information to enable detection of a wide range of potential security incident types across the entire IS. At a minimum, this configuration includes:

- Firewall
- Routers
- IDS
- Windows Logs
- Application and Service Logs
- System and Device Logs
- Spiceworks

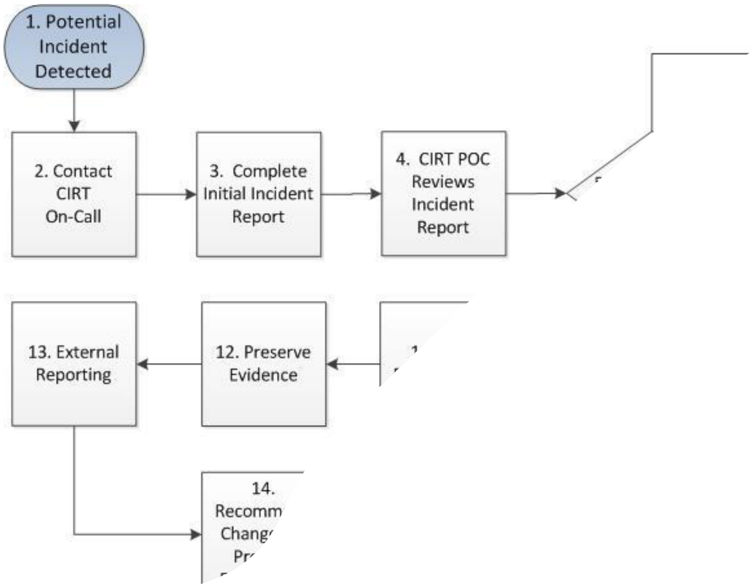
7.0.0 Continuous Monitoring Process

The System Configurations discussed in Section 6.0.0 will ensure that necessary information is available. However, these systems must be regularly monitored to allow the timely detection of potential incidents. At a minimum, this monitoring shall include:

- Spiceworks log screens are reviewed at least daily
- Information and Warning logs are reviewed at least weekly
- Critical alerts and specific error logs generate an automatic notification to on-call ITD personnel

8.0.0 Incident Response Process

Figure 1 provides a flowchart of the steps in the IR process.


1. Potential Incident Detected
2. Contact CIRT On-Call
3. Complete Initial Incident Report
4. CIRT POC Reviews Incident Report
13. External Reporting
12. Preserve Evidence
14. Recomm Chang Pr