

Incident Response Plan

Doorway

SOC 2 Criteria: CC2.2, CC2.3, CC4.2, CC5.1, CC7.3, CC7.5, CC9.1
ISO 27001 Annex A: A.16

Keywords: Impact, Security impact level, Report template, Incident

Purpose

This security incident response policy is intended to establish controls to ensure detection of security vulnerabilities and incidents, as well as quick reaction and response to security breaches.

This document also provides implementing instructions for security incident response, to include definitions, procedures, responsibilities, and performance measures (metrics and reporting mechanisms).

Scope

This policy applies to all users of information systems within Doorway. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by Doorway (hereinafter referred to as “users”). This policy must be made readily available to all users.

Background

A key objective of Doorway’s Information Security Program is to focus on detecting information security weaknesses and vulnerabilities so that incidents and breaches can be prevented wherever possible. Doorway is committed to protecting its employees, customers, and partners from illegal or damaging actions taken by others, either knowingly or unknowingly. Despite this, incidents and data breaches are likely to happen; when they do,

Doorway is committed to rapidly responding to them, which may include identifying, containing, investigating, resolving, and communicating information related to the breach.

This policy requires that all users report any perceived or actual information security vulnerability or incident as soon as possible using the contact mechanisms prescribed in this document. In addition, Doorway must employ automated scanning and reporting mechanisms that can be used to identify possible information security vulnerabilities and incidents. If a vulnerability is identified, it must be resolved within a set period of time based on its severity. If an incident is identified, it must be investigated within a set period of time based on its severity. If an incident is confirmed as a breach, a set procedure must be followed to contain, investigate, resolve, and communicate information to employees, customers, partners and other stakeholders.

Within this document, the following definitions apply:

- **Information Security Vulnerability:**

A vulnerability in an information system, information system security procedures, or administrative controls that could be exploited to gain unauthorized access to information or to disrupt critical processing.

- **Information Security Incident:**

A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of information security policy.

Roles and Responsibilities

The Security Officer is responsible for updating, reviewing, and maintaining this policy.

Policy

- All users must report any system vulnerability, incident, or event pointing to a possible incident to the Security Officer as quickly as possible but no later than 24 hours.
- Incidents must be reported by sending an email message with details of the incident.
- Users must be trained on the procedures for reporting information security incidents or discovered vulnerabilities, and their responsibilities to report such incidents. Failure to report information security incidents shall be considered to be a security violation and will be reported to the Human Resources (HR) Manager for disciplinary action.
- Information and artefacts associated with security incidents (including but not limited to files, logs, and screen captures) must be preserved in the event that they need to be used as evidence of a crime.

- All information security incidents must be responded to through the incident management procedures defined below.

Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding Doorway's expectation for them, relative to security responsibilities. The incident response plan is tested annually.

Procedure For Establishing Incident Response System:

1. Define on-call schedule and assign an Information Security Manager (ISM) responsible for managing incident response procedure during each availability window.
2. Define notification channel to alert the on-call ISM of a potential security incident. Establish a company resource that includes up to date contact information for on-call ISM.
3. Assign management sponsors from the Engineering, Legal, HR, Marketing, and C-Suite teams.
4. Distribute Procedure For Executing Incident Response to all staff and ensure up-to-date versions are accessible in a dedicated company resource.
5. Require all staff to complete training for Procedure For Executing Incident Response at least once per year.

Reporting Incidents

The following situations are to be considered for information security event reporting:

- Ineffective security control;
- Breach of information integrity, confidentiality or availability expectations;
- Human errors;
- Non-compliances with policies or guidelines;
- Breaches of physical security arrangements;
- Uncontrolled system changes;
- Malfunctions of software or hardware;
- Access violations; and,
- Malfunctions or other anomalous system behaviour indicative of a security attack or actual security breach.

Procedure For Executing Incident Response:

1. When an information security incident is identified or detected, users must notify their immediate manager within 24 hours. The manager must immediately notify the ISM on call for proper response. The following information must be included as part of the notification:
 1. Description of the incident
 2. Date, time, and location of the incident
 3. Person who discovered the incident

4. How the incident was discovered
 5. Known evidence of the incident
 6. Affected system(s)
2. Within 48 hours of the incident being reported, the ISM shall conduct a preliminary investigation and risk assessment to review and confirm the details of the incident. If the incident is confirmed, the ISM must assess the impact to Doorway and assign a severity level, which will determine the level of remediation effort required:
 1. **High:** the incident is potentially catastrophic to Doorway and/or disrupts Doorway's day-to-day operations; a violation of legal, regulatory or contractual requirements is likely.
 2. **Medium:** the incident will cause harm to one or more business units within Doorway and/or will cause delays to a business unit's activities.
 3. **Low:** the incident is a clear violation of organizational security policy, but will not substantively impact the business.
 3. The ISM, in consultation with management sponsors, shall determine appropriate incident response activities in order to contain and resolve incidents.
 4. The ISM must take all necessary steps to preserve forensic evidence (e.g. log information, files, images) for further investigation to determine if any malicious activity has taken place. All such information must be preserved and provided to law enforcement if the incident is determined to be malicious.
 5. If the incident is deemed as High or Medium, the ISM must work with the VP Brand/Creative, General Counsel, and HR Manager to create and execute a communications plan that communicates the incident to users, the public, and others affected.
 6. The ISM must take all necessary steps to resolve the incident and recover information systems, data, and connectivity. All technical steps taken during an incident must be documented in Doorway's incident log, and must contain the following:
 1. Description of the incident
 2. Incident severity level
 3. Root cause (e.g. source address, website malware, vulnerability)
 4. Evidence
 5. Mitigations applied (e.g. patch, re-image)
 6. Status (open, closed, archived)
 7. Disclosures (parties to which the details of this incident were disclosed to, such as customers, vendors, law enforcement, etc.)
 7. After an incident has been resolved, the ISM must conduct a post-mortem that includes root cause analysis and documentation of any lessons learned.
 8. Depending on the severity of the incident, the Chief Executive Officer (CEO) may elect to contact external authorities, including but not limited to law enforcement, private investigation firms, and government organizations as part of the response to the incident.
 9. The ISM must notify all users of the incident, conduct additional training if necessary, and present any lessons learned to prevent future occurrences. Where necessary, the HR Manager must take disciplinary action if a user's activity is deemed as malicious.

Appendix A: Security Incident Report Template

1.0 Reported By

1.1 Last Name:	
1.2 First Name:	
1.3 Position:	
1.4 Company/Org Name:	
1.5 Telephone No:	
1.6 E-mail:	

2.0 Organization Details

2.1 Name of organisation:	
2.2 Type of organisation:	
2.3 Street Address:	
2.4 At this time, is it known that other organisations are affected by this incident? (If so, list names, addresses, telephone number, email addresses and contact persons):	

3.0 Incident Details including Injury and Impact Level

3.1 Date:	3.2 Time:	
3.3 Location of affected site:		
3.4 Brief summary of the incident (what		

has happened, where did it happen, when did it happen):	
3.5 Description of the project/program and information involved, and, if applicable, the name of the specific program:	
3.6 Classification level of the information involved	
3.7 System compromise (detail):	
3.8 Data compromise (detail):	
3.9 Originator and /or Official Classification Authority of the information involved? (List name, address, telephone no., email and contact person).	
3.10 Is Foreign Government Information involved? Originating country or International organisation?	
3.11 Did the incident occur on an accredited system authorised to process and store the information in question?	
3.12 Estimated injury level/sector:	
3.13 Estimated impact level: (any compromise or disruption to service?)	
3.14 Incident duration:	
3.15 Estimated number of systems affected:	
3.16 Percentage of organisation systems affected:	
3.17 Action taken:	
3.18 Supporting documents attached (describe if any)	
3.19 Multiple occurrence or first time this type of incident occurs within this location?	
3.20 Incident Status (resolved or unresolved)	
3.21 Has the matter been reported to other authorities? If so, list names, addresses, telephone no., email and contact person.	

4.0 Status of Mitigation Actions

4.1 Mitigation details to date: (List any actions that have been taken to mitigate incident and by whom)	
4.2 Results of mitigation:	
4.3 Additional assistance required?	

5.0 Computer Network Defense Incident Type (if applicable)

5.1 Malicious code: (Worm, virus, trojan, backdoor, rootkit, etc.)				
5.2 Known vulnerability exploit: (List the Common Vulnerabilities and Exposures (CVE) number for known vulnerability)				
5.3 Disruption of service:				
5.4 Access violation: (Unauthorised access attempt, successful unauthorised access, password cracking, Etc.)				
5.5 Accident or error: (Equipment failure, operator error, user error, natural or accidental causes)				
5.6 If the incident resulted from user error or malfeasance, identify reasons (training, disregard for policy, other) and responsible parties				
5.7 Additional details:				
5.8. Apparent Origin of Incident or Attack	Source IP and port:		Protocol:	
	URL:		Malware:	
	Additional details:			

6.0 Systems Affected

--	--

6.1 Network zone affected: (Internet, administration, internal, etc.)	
6.2 Type of system affected: (File server, Web server, mail server, database, workstation (mobile or desktop), etc.)	
6.3 Operating system (specify version):	
6.4 Protocols or services:	
6.5 Application (specify version):	

7.0 Post Incident Activities

7.1 Has information contained in this report been provided to the authorities? When?	
7.2 Complete a root cause analysis to determine the reason for the incident and steps to prevent re-occurrence.	

Revision History

--	--	--	--

Version	Date	Editor	Description of Changes
1.0	24.02.2022	Henry Sinclair	Initial Creation