Incident Response Plan

Nave

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

Background

A key objective of Nave’s Information Security Program is to focus on detecting information security weaknesses and vulnerabilities so that incidents and breaches can be prevented wherever possible. Nave 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, Nave 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, Nave 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.

- Information Security Event:
  An occurrence or change in the normal behavior of systems, networks or services that may impact security and organizational operations (e.g., possible compromise of policies or failure of controls).

Roles and Responsibilities

This Policy is maintained by Nave Security Officer and Privacy Officer.

The incident handler is responsible for verifying alerts, initiating containment actions, performing forensic analysis, determining whether the incident constitutes a breach, coordinating with system administrators, preparing the final incident report, and ensuring compliance with required evidence retention periods.

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.
- Employees who suspect accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data must immediately report the situation to the designated incident handler at sonya@getnave.com. Once notified, the incident handler will alert local system administrators and initiate appropriate containment procedures.
- 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 artifacts associated with security incidents (including but not limited to files, logs, and screen captures) must be preserved appropriately 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 Nave's expectation for them, relative to security responsibilities. The incident response plan is tested annually.

Procedure For Establishing Incident Response System

- 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:
    - Description of the incident
    - Date, time, and location of the incident
    - Person who discovered the incident
    - How the incident was discovered
    - Known evidence of the incident
    - Affected system(s)
- If a compromised host cannot immediately be removed from the network, the incident handler will initiate a full-content network dump to monitor the attacker's activities and determine whether any data is leaking.
- The incident handler will also implement network quarantine at the time of detection whenever possible, and coordinate with system administrators to gather a preliminary list of compromised components, affected storage media, and an initial attack timeline.
- 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 Nave and assign a severity level, which will determine the level of remediation effort required:
    - **High:** the incident is potentially catastrophic to Nave and/or disrupts Nave's day-to-day operations; a violation of legal, regulatory or contractual requirements is likely.
    - **Medium:** the incident will cause harm to one or more business units within Nave and/or will cause delays to a business unit's activities.
    - **Low:** the incident is a clear violation of organizational security policy, but will not substantively impact the business.
- To determine whether the incident qualifies as a breach, the incident handler will assess the following:
    - Whether suspicious network traffic indicates potential data exfiltration
    - Whether attackers had privileges enabling access to sensitive data
    - Whether encryption prevented unauthorized reading
    - Availability of file-access audit logs showing access after compromise
    - Duration of compromise and attacker activities
    - Whether tools used by the attacker are capable of locating or exfiltrating data
    - Any indicators that information was downloaded, copied, used, or is in possession of an unauthorized party
- The ISM, in consultation with management sponsors, shall determine appropriate incident response activities in order to contain and resolve incidents.
- 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. The collection of evidence will be managed by appropriate members with proper understanding and training in forensic evidence collection. In the absence of such members, certified third-party professionals will be used. All

such information must be preserved and provided to law enforcement if the incident is determined to be malicious.

- During the analysis phase, the incident handler will conduct an in-depth review of all network-based and host-based evidence to determine attacker actions, establish an attack timeline, and assess whether any data was successfully accessed or exfiltrated. A peer review of the analysis must be performed by technical staff before the final incident report is written.
- 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.
- 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 Nave's incident log, and must contain the following:
    - Description of the incident
    - Incident severity level
    - Root cause (e.g. source address, website malware, vulnerability)
    - Evidence
    - Mitigations applied (e.g. patch, re-image)
    - Status (open, closed, archived)
    - Disclosures (parties to which the details of this incident were disclosed to, such as customers, vendors, law enforcement, etc.)
- Compromised systems must be fully remediated before network quarantine is lifted. This includes confirming that attacker access has been completely eliminated and all vulnerabilities have been addressed.
- After an incident has been resolved, the ISM must conduct a post-mortem that includes root cause analysis and documentation of any lessons learned.
    - In the event that the incident involves the breach of sensitive privacy data (e.g., PII), (1) an assessment will also be conducted to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected parties; (2) all affected parties and appropriate organizations (e.g., Law Enforcement) will be notified; and (3) every effort will be made to mitigate the harm to affected parties.
- The final incident report must also include mid-term and long-term recommendations for improvements in technology or business processes to reduce operating risk and prevent future occurrences.
- 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.
- 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.

Incident Documentation Retention

Final incident reports must be retained for six (6) years. Incident notes and processed investigation materials must be retained for six (6) months from the date the final report is issued.

Raw incident data must be retained for thirty (30) days from the date the final report is issued.

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 organization:	
2.2 Type of organization:	
2.3 Street Address:	
2.4 At this time, is it known that other organizations are affected by this incident? (If so, list names, addresses, telephone number, email addresses & 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 organization?	

3.11 Did the incident occur on an accredited system authorized 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 organization systems affected:	
3.17 Action taken:	
3.18 Supporting documents attached (describe if any)	
3.19 Multiple occurrences 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 (Unauthorized access attempt, successful unauthorized 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, 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:	
	URL:	
	Protocol:	
	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	Approver	Description of Changes
1.0	02/13/2024	Rhymetec	Taha Oualif	Initial policy creation

1.1	02/13/2025	VG	Taha Oualif	Annual Update