Incident Management and Response

Purpose

This Incident Response Plan exists to ensure that we consistently handle information security events in an effective and efficient manner.

Scope

This policy offers guidance for employees, contractors, and consultants of Nested Knowledge who believe they have discovered or are responding to a security incident.

Affected Systems

This policy applies to all computer and communication systems owned or operated by Nested Knowledge and its subsidiaries. Systems include company shared drives, purchased software, as well as access to the Nested Knowledge AutoLit review platform. Reviews developed in the AutoLit software by parties external to Nested Knowledge are not covered in this policy.

Incidence Response Plan

The incident response (IR) team will consist of the following personnel:

- Karl Holub, technical lead
- Kevin Kallmes, CEO; investigator
- Kathryn Cowie, operations lead; investigator
- Other incident responders may be assigned as needed.

Risk Register

Nested Knowledge Incidence Response Team will maintain a list of security threats and vulnerabilities, classified by likelihood and consequence.

Asset	Threat/Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
Workstations	Malicious files/ processes Unprotected data	Security policy dissemination and training	Highly Possible	Major	Very High

Asset	Threat/Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
NK Application	Injection, privilege escalation, leaks, untrustworthy dependencies	Runtime environment restrictions, mandated code review, dependency locking, developer education, penetration testing	Possible	Major	High
Databases	Compromised access, through brute force or leaks	Network Isolation, key-based authentication, regular off-site backups	Possible	Major	High
Servers	Compromised access, through brute force or leaks	Network Isolation, key-based authentication	Possible	Minor	Low

ii) Incident Reporting

Detection and Reporting

When an incident is detected, Nested Knowledge personnel should behave as if they reporting a crime and include lots of specific details about what they have discovered.

Nested Knowledge has prepared an incident response form for use while investigating an incident. Nested Knowledge Employees and contractors will be provided with access to the form and instructed to utilize it for all suspected incidents. The IR team will monitor responses and react immediately upon receipt.

In addition to submitting details via the form, Nested Knowledge personnel must email karl.holub@nested-knowledge.com or send a message to #incident-response to notify the security team of suspected issues.

Reporting a Data Breach

For breachs likely to result in a risk to users or employees, Nseted Knowledge will notify a Supervisory Authority within 72 hours with:

- categories of data and the number of data subjects affected
- our DPO's contact information
- likely consquences of the breach
- measures proposed and taken to address the breach

Reporting Scams to Authorities

You can report scams, phishing attempts, and other cyber incidents to:

- The FBI's Internet Crime Complaint Center
- The FTC
    - Forward emails to reportphishing@apwg.org.
    - Forward texts to SPAM (7726)

Internal Issues

Issues where the malicious actor is an internal employee, contractor, vendor, or partner requires sensitive handling. Please contact the CEO and CTO directly. These are critical issues and must be pushed to follow up.

iii) Incident Categorization

We categorize incidents by severity and scope of control.

Severity

Low-Medium Severity

Issues meeting this severity are simply suspicions or odd behaviors. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do not require emergency response. This includes suspicious emails, outages, strange activity on a laptop.

High Severity

High severity issues relate to problems where an active exploitation hasn’t been proven, but is likely to happen. This include vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (eg: backdoors, malware), malicious access of business data (eg: passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm.

High severity issues should include an email to karl.holub@nested-knowledge.com with “Urgent” in the subject line, or a message to #info-sec with “@channel” in the message to alert incident responders.

Critical Severity

Critical issues relate to actively exploited risks and involve a malicious actor. Critical severity issues should involve a message to “@channel” in #info-sec. Continue escalation until you receive

acknowledgement. Involvement of a crisis lead and a lawyer are highly recommended.

Scope of Control

Incidents may be triggered by events that are inside or outside our scope of control.

External Risk Events

- Supplier incident - service compromise, breach or unavailability
- Regulatory change - unforeseen rules change
- Security research - critical vulnerability published

Internal Risk Events

- Abusive content - harmful, child, sexual or violent speech or content, harassment
- Malware - ransomware, worm, spyware, rootkits, etc
- Availability interruption - denial of service or sabotage
- Information gathering - reconnaissance activities, network scanning or sniffing
- Social engineering - phishing, bribes and other (physical) threats
- Information breach - unauthorised access to, or sharing, modification or deletion of system/information
- Fraud - theft of money or misappropriation of company resources
- System intrusion - software exploit, SQL injection, XSS, use of stolen credentials
- Governance failure - process or audit failure

iv) Coordinating a Response

We primarily use Slack to coordinate our response to cyber security events. We also use Google Meets call for response update calls. If an issue is classified as Critical Severity we will create a channel in Slack specifically for that issue and include the relevant individuals and assign roles at that time. Phone numbers, email and other details on individuals and our key suppliers can be found in Key Contacts.

v) Incidence Response

For critical issues, the incidence response team will follow an iterative response process designed to investigate, contain exploitation, remediate our vulnerability, and document a post-mortem with the lessons of an incident.

1. Observe/Orient
    1. - The technical lead and investigators will collect relevant data. Contextual information, such as asset information, company plans, and external/open-source intelligence may be used to help understand the landscape.
2. Decide

    1. The operations lead will record decisions and justifications for the selected course of action.
    2. The technical lead and CEO will determine if a lawyer should be included and attorney client privilege between responders will begin.
3. Act
    1. The technical lead, with support from other personnel, acts on the decisions made in the previous stage to further the investigation or remedy of the situation.
    2. A meeting will occur at regular intervals until the incident is resolved.
4. Review
    1. Post-incident reviews are conducted without blame or finger-pointing to encourage open and honest participation so that lessons can be learned and improvements identified. Failing to create the right open, safe environment may cause participants to withhold information crucial to preventing events from occurring again.
5. Recover
    1. Business as usual will be restored as soon as feasible. For more details on recovery, please see the Business Continuity Policy

Data Sources

The Technical Lead and Investigators are responsible for capturing and collating data that support the investigation of a security incident.Data and logs should be sourced from Data Sources relevant to the investigation

Potential Data Sources

- Account activity - domain controller and active directory logs
- IT Assets
- Software configuration (authorized software packages)
- Web logs and potentially similar host logs to above
- Information storage (document management systems and databases)
- Financial systems
- Cloud service-specific logs
- Local system activity

Mitigation Process due to Information Loss

Data lost or stolen must be taken into account, complying with state and federal laws mentioned in Part 1.

- PII loss will be notified to the concerned persons as well as government authorities.
- Incident will be analyzed, and action will be taken if evidence of transgressions by an employee is found. Legal team must assess the repercussions due to the loss, and will provide an official statement to the management regarding potential compensation losses to be incurred.

Specific Plans for loss of Availability of Services:

- Databases protected with credentials. Primary and secondary servers are allocated for

databases, to make sure services available even if a server is down. Databases are backed up by our cloud services provider on a transaction level and periodically exported to a different provider.
- Servers are protected and backed-up by our cloud services provider, who provide coverage and consistent working, even during blackouts, shutdowns etc.
- Laptops and Mobiles which are lost or compromised, cannot access our network without multi-factor authentication.

Key Contacts

Name	Function	Contact
Kevin Kallmes	CEO - critical decisions, public relations	kevinkallmes@supedit.com
Karl Holub	CTO - technical lead	karl.holub@nested-knowledge.com
Kathryn Cowie	COO - coordination, documenting response an decisions	kathryn.cowie@nested-knowledge.com
John Fallone	Lawyer - legal assistance	john@fallonesv.com
Dr. Dheerendra	Board Member	dkommala@ecri.com

Security Incidents

[Example]

Timestamp	Event	Description	Reported By	Status
01-17-2023 10:34 ET	Phishing email	Fraudulent email requesting payroll: moved to SPAM, blocked sender, and deleted.	Kathryn Cowie	Resolved 01-17-2023 10:37 ET

Revision History

Author	Date of Revision/Review	Comments
K. Cowie	11/15/2021	Initial draft in progress; risk register needs technical review.
K. Kallmes	11/19/2021	Draft approved
K. Holub	09/30/2022	Reviewed with grammar edits
P. Olaniran	9/29/2022	Minor revisions

Return to Policies

Risk Register

Nested Knowledge Incidence Response Team will maintain a list of security threats and vulnerabilities, classified by likelihood and consequence.

Asset	Threat/Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk
Workstations	Malicious files/ processes Unprotected data	Security policy dissemination and training	Highly Possible	Major	Very High
NK Application	Injection, privilege escalation, leaks, untrustworthy dependencies	Runtime environment restrictions, mandated code review, dependency locking, developer education, penetration testing	Possible	Major	High
Databases	Compromised access, through brute force or leaks	Network Isolation, key-based authentication, regular off-site backups	Possible	Major	High
Servers	Compromised access, through brute force or leaks	Network Isolation, key-based authentication	Possible	Minor	Low

ii) Incident Reporting

Detection and Reporting

When an incident is detected, Nested Knowledge personnel should behave as if they reporting a crime and include lots of specific details about what they have discovered.

Nested Knowledge has prepared an incident response form for use while investigating an incident. Nested Knowledge Employees and contractors will be provided with access to the form and instructed to utilize it for all suspected incidents. The IR team will monitor responses and react immediately upon receipt.

In addition to submitting details via the form, Nested Knowledge personnel must email karl.holub@nested-knowledge.com or send a message to #incident-response to notify the security team of suspected issues.

Reporting a Data Breach

For breachs likely to result in a risk to users or employees, Nseted Knowledge will notify a Supervisory Authority within 72 hours with:

- categories of data and the number of data subjects affected
- our DPO's contact information
- likely consquences of the breach
- measures proposed and taken to address the breach

Reporting Scams to Authorities

You can report scams, phishing attempts, and other cyber incidents to:

- The FBI's Internet Crime Complaint Center
- The FTC
    - Forward emails to reportphishing@apwg.org.
    - Forward texts to SPAM (7726)

Internal Issues

Issues where the malicious actor is an internal employee, contractor, vendor, or partner requires sensitive handling. Please contact the CEO and CTO directly. These are critical issues and must be pushed to follow up.

iii) Incident Categorization

We categorize incidents by severity and scope of control.

Severity

Low-Medium Severity

Issues meeting this severity are simply suspicions or odd behaviors. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do not require emergency response. This includes suspicious emails, outages, strange activity on a laptop.

High Severity

High severity issues relate to problems where an active exploitation hasn't been proven, but is likely to happen. This include vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (eg: backdoors, malware), malicious access of business data (eg: passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm.

High severity issues should include an email to karl.holub@nested-knowledge.com with "Urgent" in the subject line, or a message to #info-sec with "@channel" in the message to alert incident responders.

Critical Severity

Critical issues relate to actively exploited risks and involve a malicious actor. Critical severity issues

should involve a message to “@channel” in #info-sec. Continue escalation until you receive acknowledgement. Involvement of a crisis lead and a lawyer are highly recommended.

Scope of Control

Incidents may be triggered by events that are inside or outside our scope of control.

External Risk Events

- Supplier incident - service compromise, breach or unavailability
- Regulatory change - unforeseen rules change
- Security research - critical vulnerability published

Internal Risk Events

- Abusive content - harmful, child, sexual or violent speech or content, harassment
- Malware - ransomware, worm, spyware, rootkits, etc
- Availability interruption - denial of service or sabotage
- Information gathering - reconnaissance activities, network scanning or sniffing
- Social engineering - phishing, bribes and other (physical) threats
- Information breach - unauthorised access to, or sharing, modification or deletion of system/information
- Fraud - theft of money or misappropriation of company resources
- System intrusion - software exploit, SQL injection, XSS, use of stolen credentials
- Governance failure - process or audit failure

iv) Coordinating a Response

We primarily use Slack to coordinate our response to cyber security events. We also use Google Meets call for response update calls. If an issue is classified as Critical Severity we will create a channel in Slack specifically for that issue and include the relevant individuals and assign roles at that time. Phone numbers, email and other details on individuals and our key suppliers can be found in Key Contacts.

v) Incidence Response

For critical issues, the incidence response team will follow an iterative response process designed to investigate, contain exploitation, remediate our vulnerability, and document a post-mortem with the lessons of an incident.

1. Observe/Orient
    1. - The technical lead and investigators will collect relevant data. Contextual information, such as asset information, company plans, and external/open-source intelligence may be used to help understand the landscape.

2. Decide
    1. The operations lead will record decisions and justifications for the selected course of action.
    2. The technical lead and CEO will determine if a lawyer should be included and attorney client privilege between responders will begin.
3. Act
    1. The technical lead, with support from other personnel, acts on the decisions made in the previous stage to further the investigation or remedy of the situation.
    2. A meeting will occur at regular intervals until the incident is resolved.
4. Review
    1. Post-incident reviews are conducted without blame or finger-pointing to encourage open and honest participation so that lessons can be learned and improvements identified. Failing to create the right open, safe environment may cause participants to withhold information crucial to preventing events from occurring again.
5. Recover
    1. Business as usual will be restored as soon as feasible. For more details on recovery, please see the Business Continuity Policy

Data Sources

The Technical Lead and Investigators are responsible for capturing and collating data that support the investigation of a security incident.Data and logs should be sourced from Data Sources relevant to the investigation

Potential Data Sources

- Account activity - domain controller and active directory logs
- IT Assets
- Software configuration (authorized software packages)
- Web logs and potentially similar host logs to above
- Information storage (document management systems and databases)
- Financial systems
- Cloud service-specific logs
- Local system activity

Mitigation Process due to Information Loss

Data lost or stolen must be taken into account, complying with state and federal laws mentioned in Part 1.

- PII loss will be notified to the concerned persons as well as government authorities.
- Incident will be analyzed, and action will be taken if evidence of transgressions by an employee is found. Legal team must assess the repercussions due to the loss, and will provide an official statement to the management regarding potential compensation losses to be incurred.

Specific Plans for loss of Availability of Services:

- Databases protected with credentials. Primary and secondary servers are allocated for databases, to make sure services available even if a server is down. Databases are backed up by our cloud services provider on a transaction level and periodically exported to a different provider.
- Servers are protected and backed-up by our cloud services provider, who provide coverage and consistent working, even during blackouts, shutdowns etc.
- Laptops and Mobiles which are lost or compromised, cannot access our network without multi-factor authentication.

Key Contacts

Name	Function	Contact
Kevin Kallmes	CEO - critical decisions, public relations	kevinkallmes@supedit.com
Karl Holub	CTO - technical lead	karl.holub@nested-knowledge.com
Kathryn Cowie	COO - coordination, documenting response an decisions	kathryn.cowie@nested-knowledge.com
John Fallone	Lawyer - legal assistance	john@fallonesv.com

Security Incidents

[Example]

Timestamp	Event	Description	Reported By	Status
01-17-2023 10:34 ET	Phishing email	Fraudulent email requesting payroll: moved to SPAM, blocked sender, and deleted.	Kathryn Cowie	Resolved 01-17-2023 10:37 ET

Revision History

Author	Date of Revision/Review	Comments
K. Cowie	11/15/2021	Initial draft in progress; risk register needs technical review.
K. Kallmes	11/19/2021	Draft approved
K. Holub	09/30/2022	Reviewed with grammar edits
P. Olaniran	9/29/2022	Minor revisions

Return to Policies