nebul

CUSTOMER DATA INCIDENT RESPONSE PROCESS

Nebul's highest priority is to maintain a safe and secure environment for Customer Data. Nebul's security policies and systems may change going forward, as we continually improve protection for Customer.

Table of Contents

INTRODUCTION

Nebul's highest priority is to maintain a safe and secure environment for Customer Data. To help protect Customer Data, we run an industry-leading information security operation that combines stringent processes, an expert incident response team, and multi-layered information security and privacy infrastructure. This document explains our principled approach to managing and responding to any breach of Nebul's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Nebul ("Customer Data Incidents"). Any capitalized terms used in this document have the definitions given in Schedule 1 of the Data Processing Addendum and Schedule 1 of the Master Agreement.

While we take steps to address foreseeable threats to data and systems, Customer Data Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Data. For example, Customer Data Incidents are not unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems. Please note that Section 7 of the Data Processing Addendum applies in addition to and prevails over this document to the extent of any conflict, if a Customer Data Incident qualifies as a Personal Data Incident within the meaning of the Data Processing Addendum.

Incident response is a key aspect of our overall security and privacy program. We have a rigorous process for managing Customer Data Incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any incidents that impact the confidentiality, integrity, or availability of Customer Data.

NOTIFICATION

Any Customer Data Incident notifications must be sent to Nebul security in deviation of Section 12.10.2 of the Master Agreement. The email address is: security@nebul.com.

CUSTOMER DATA INCIDENT RESPONSE

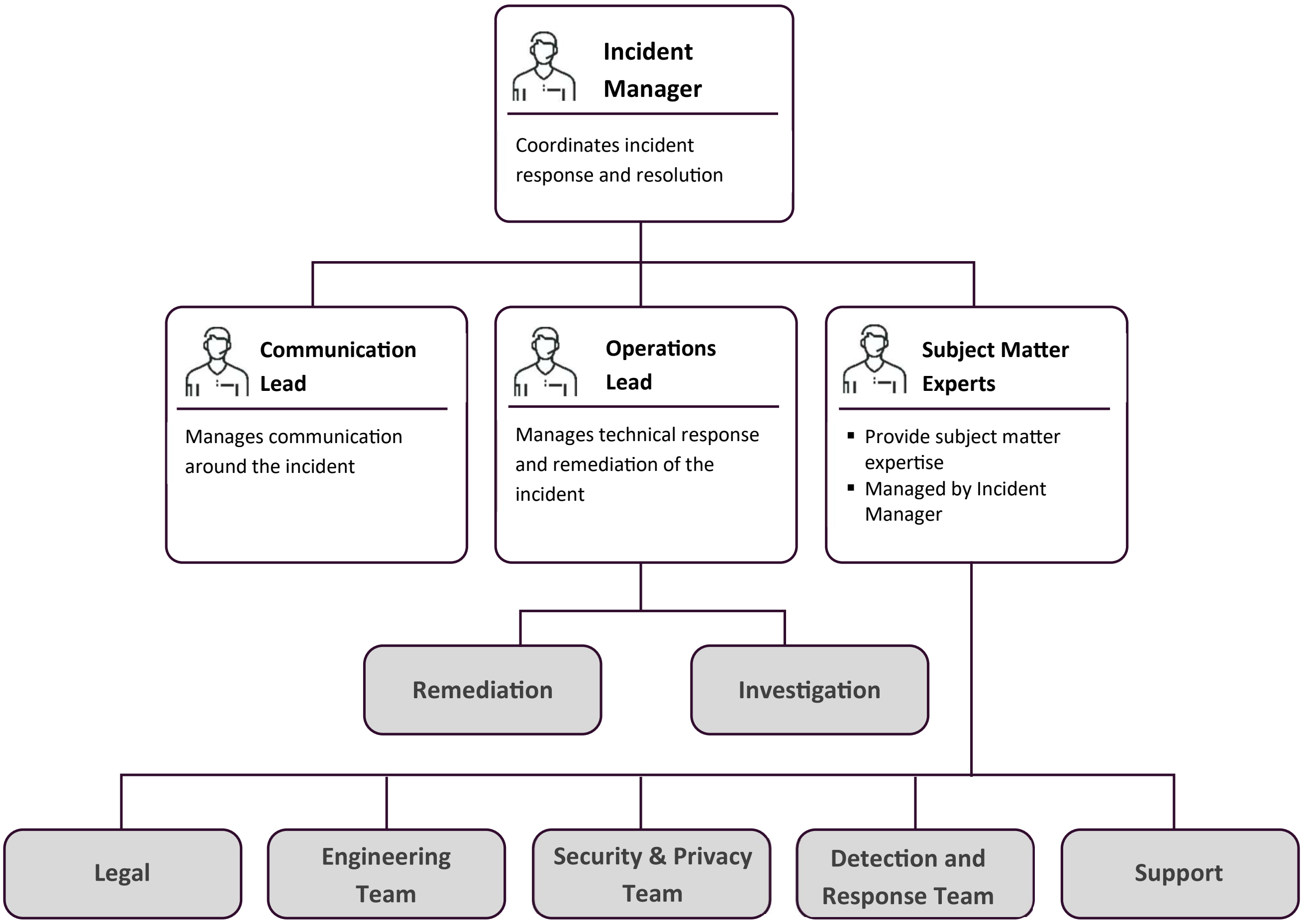
Depending on the nature of the Customer Data Incident, the professional Nebul's Customer Data Incident response team might include people from the following teams:

- Support team (Incident and escalation management)
- Monitoring, detection and response
- Security and privacy
- Engineering
- External experts

People from these teams are engaged in a variety of ways. For example, incident managers coordinate incident response and, when needed, the digital forensics team performs forensic investigations and tracks ongoing Customer Data Incidents. Product engineers work to limit the impact on Customers and provide solutions to fix the affected products. Counsel works with members of the appropriate security and privacy team to implement Nebul's strategy on evidence collection, engage with law enforcement and government regulators, and advise on legal issues and requirements. Customer care responds to Customer inquiries and requests for additional information and assistance.

TEAM ORGANIZATION

When we declare a Customer Data Incident, we designate an incident manager who coordinates Customer Data Incident response and resolution. The incident manager selects specialists from different teams and forms a response team ("Incident Response Team"). The incident manager delegates the responsibility for managing different aspects of the Customer Data Incident to these experts and manages the Customer Data Incident from the moment of declaration to closure. The following diagram depicts an example of an Incident Response Team, including the various roles and their responsibilities during Customer Data Incident response. Depending on the type of Customer Data Incident, different roles might be assigned.


Incident Manager
Coordinates incident response and resolution
Communication Lead
Manages communication around the incident
Operations Lead
Manages technical response and remediation of the incident
Subject Matter Experts
▪ Provide subject matter expertise
▪ Managed by Incident Manager
Remediation
Investigation
Legal
Engineering Team
Security & Privacy Team
Detection and Response Team
Support

CUSTOMER DATA INCIDENT RESPONSE PROCESS

Every Customer Data Incident is unique, and Nebul's goal is to protect Customer Data, restore normal service as quickly as possible, and meet both legal and contractual requirements. The following table describes the main steps in Nebul's Customer Data Incident response ("Customer Data Incident Response Process"). Note that multiple steps may be taken simultaneously.

Incident step	Goal	Description
Identification	Detection	Automated and manual processes detect potential vulnerabilities and Customer Data Incidents.
	Reporting	Automated and manual processes report the issue to the Incident Response Team.
Coordination	Triage	The following activities occur: ▪ On-call responder evaluates the nature of the incident report. ▪ On-call responder assesses severity of the incident. ▪ On-call responder escalates to incident manager
	Incident Response Team engagement	The following activities occur: ▪ Incident manager completes assessment of known facts. ▪ Incident manager designates leads from relevant teams and forms Incident Response Team. ▪ Incident Response Team evaluates incident and response effort.
Resolution	Investigation	The following activities occur: ▪ Incident Response Team gathers key facts about the incident. ▪ Additional resources are integrated as needed to allow for expedient resolution.
	Containment and recovery	Operations lead takes steps to complete the following: ▪ Limit ongoing damage. ▪ Fix underlying issue ▪ Restore affected systems and Services to normal operations.
	Communication	The following activities occur: ▪ Key facts are evaluated to determine whether notification to the Supervisory Authority and/or data subject is appropriate. ▪ Report of the investigation regarding the Customer Data Incident is shared with Customer. ▪ Communication lead develops a communication plan with appropriate leads.
Closure	Lessons learned	The following activities occur: ▪ Incident Response Team retrospects on incident and response effort. ▪ Incident management designates owners for long-term improvements.
Continuous improvement	Program development	Necessary teams, training, processes, resources, and tools are maintained.
	Prevention	Teams improve the Customer Data Incident Response Process based on lessons learned.

The following sections describe each step in more detail.

IDENTIFICATION

Early and accurate identification of incidents is key to effective incident management. The focus of the identification phase is to monitor security events to detect and report on potential Customer Data Incidents.

The incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential Customer Data Incidents. Our sources of incident detection include the following:

- **Automated network and system logs analysis:** Automated analysis of network traffic and system access helps identify suspicious, abusive, or unauthorized activity and escalates to security staff.
- **Testing:** The security team actively scans for security threats using penetration tests, quality assurance (QA) measures, intrusion detection, and software security reviews.
- **Internal code reviews:** Source code review discovers hidden vulnerabilities, design flaws, and verifies if key security controls are implemented.
- **Product-specific tooling and processes:** Automated tooling specific to the team function is employed wherever possible to enhance our ability to detect incidents at product level.
- **Usage anomaly detection:** We use layers of machine learning systems to differentiate between safe and anomalous user activity across different datacenter services and other usage events.
- **Data center and workplace services security alerts:** Security alerts in data centers scan for incidents that might affect our infrastructure.
- **Nebul employees:** A Nebul employee detects an anomaly and reports it.
- **Nebul’s vulnerability reward program:** Potential technical vulnerabilities in Services that affect the confidentiality or integrity of Customer Data can be reported by external security researchers.
- **Notifications from 3rd parties:** Nebul has created a process to receive, review and act upon third-party notifications.

COORDINATION

When an incident is reported, the on-call responder reviews and evaluates the nature of the incident report to determine if it represents a Customer Data Incident, including potential Customer Data Incidents, and initiates our Customer Data Incident Response process.

After confirmation, the responder assesses the nature of the Customer Data Incident and implements a coordinated approach to the response. At this stage, the response includes completing the triage assessment of the Customer Data Incident, adjusting its severity if required, and activating the required incident response team with appropriate operational and technical leads who review the facts and identify key areas that require investigation. We designate a product lead and a legal lead to make key decisions on how to respond. The responder then assigns the responsibility for investigation and the facts are assembled. If necessary, a Customer Data Incident is declared and an incident manager is assigned.

Many aspects of our response depend on the assessment of severity, which is based on key facts that are gathered and analyzed by the Incident Response Team. These key facts include the following:

- Evaluation of the risk and potential for harm to Customers, third parties, and Nebul
- Nature of the Customer Data Incident (for example, whether data was potentially destroyed, accessed, or altered)
- Type of Customer Data that might be affected
- Impact of the Customer Data Incident on our Customers’ ability to use the Service
- Status of the Customer Data Incident (for example, whether the incident is isolated, continuing, or contained)

The incident manager and other leads periodically re-evaluate these factors throughout the response effort as new information evolves to ensure that our response is assigned the appropriate resources and urgency. Events that present the most critical impact are assigned the highest severity. A communication lead is appointed to develop a communications plan with other leads.

INCIDENT SEVERITY CLASSIFICATION

Critical (Level 1)
Severe security incidents with immediate and significant impact on Customer Data, systems, or reputation.

Examples:

- Confirmed data breach of sensitive Customer Data
- Active cyber-attack with potential for significant data loss
- Widespread malware infection affecting critical systems
- Insider threat actions with severe potential impact

Response and execution of work:

- First response and triage within 15 minutes
- Continuous work until containment is achieved (24x7x365)
- Status updates to stakeholders every 2 hours

High (Level 2)
Serious security incidents with potential for significant impact if not addressed quickly.

Examples:

- Suspected data breach in Nebul systems, extent unknown
- Targeted phishing attack on specific customer environment
- Compromised admin credentials
- Denial of Service (DoS) attack impacting critical Nebul Cloud services

Response and execution of work:

- First response and triage within 1 hour
- Continuous work until containment is achieved (24x7x365)
- Status updates to stakeholders every 4 hours

Medium (Level 3)
Moderate security incidents that require attention but do not pose an immediate threat to critical assets.

Examples:

- Isolated malware infection of Nebul Systems
- Unauthorized access attempts to sensitive Nebul systems
- Lost or stolen device containing sensitive data
- Moderate policy violations with security implications

Response and execution of work:

- First response and triage within 4 hours during Business Days
- Work progresses during business hours until resolution
- Daily status updates to stakeholders

Low (Level 4)
Minor security incidents or potential issues that should be logged and addressed as part of regular operations.

Examples:

- Minor policy violations
- Isolated phishing attempts
- Suspected but unconfirmed security anomalies
- Low-impact vulnerabilities discovered in non-critical systems

Response and execution of work:

- First response and triage within 1 Business Day
- Work addressed as part of regular security operations
- Status updates as part of weekly security reports

Escalation
The response times given for each incident severity class are based on best efforts and are indicative only. Critical and High incidents require immediate notification to the Chief Information Security Officer (CISO) or designated Officer.

RESOLUTION

At the resolution stage, the focus is on investigating the root cause, limiting the impact of the Customer Data Incident, resolving immediate security risks (if any), implementing necessary fixes as part of remediation, and recovering affected systems, Customer Data, and Services.

Affected Customer Data is restored to its original state wherever possible. Depending on what is reasonable and necessary in a particular Customer Data Incident, we might take a number of different steps to resolve a Customer Data Incident. For instance, there might be a need for technical or forensic investigation to reconstruct the root cause of an issue or to identify any impact on Customer Data. We might attempt to recover copies of Customer Data from our backup copies if it is improperly altered or destroyed.

A key aspect of remediation is notifying Customers when Customer Data Incidents impact their Customer Data. Key facts are evaluated throughout the Customer Data Incident to determine whether Customer Data is affected. If notifying Customer is required, the incident manager initiates the notification process. A report of the investigation on the Customer Data Incident and the findings will be shared with Customer (with the exception of Nebul Confidential Information). The communications lead develops a communication plan with input from the product and legal leads, informs those affected, and supports Customer requests after notification. It is the Customer's exclusive responsibility to assess whether a Customer Data Incident must be reported to third parties (e.g., Supervisory Authorities, affected individuals or, if Customer is a processor and the Customer Data Incident qualifies as a Personal Data Incident, the controller).

We strive to provide prompt, clear, and accurate notifications containing the known details of the Customer Data Incident, steps that we have taken to mitigate the potential risks, and actions that we recommend Customer take to address the Customer Data Incident. We do our best to provide a clear picture of the Customer Data Incident so that Customer can assess and fulfill their own obligations under Applicable Law.

CLOSURE

Following the successful remediation and resolution of a Customer Data Incident, the Incident Response Team evaluates the lessons learned from the Customer Data Incident. When the Customer Data Incident raises critical issues, the incident manager might initiate a post-mortem analysis. During this process, the Incident Response Team reviews the causes of the Customer Data Incident and our Customer Data Incident Response Process and identifies key areas for improvement. In some cases, this might require discussions with different product, engineering, and operations teams and product enhancement work. If follow-up work is required, the Incident Response Team develops an action plan to complete that work and assigns project managers to lead the long-term effort. The Customer Data Incident Response Process is closed after the remediation efforts are concluded.

CONTINUOUS IMPROVEMENT

Nebul strives to learn from every Customer Data Incident and implement preventative measures to avoid future Customer Data Incidents. Actionable insights from Customer Data Incident analysis enable us to enhance our tools, training, processes, overall security and privacy data protection program, security policies, and response efforts. The key learnings also facilitate prioritization of engineering efforts and building of better products.

Security and privacy professionals enhance our program by reviewing our security plans for all networks, systems, and services, and by providing project-specific consulting services to product and engineering teams. Security and privacy professionals deploy machine learning, data analysis, and other novel techniques to monitor for suspicious activity on our networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments.

We conduct regular training and awareness campaigns to drive innovation in security and data privacy. Dedicated incident response staff are trained in forensics and in handling evidence, including the use of third-party and proprietary tools. Testing of the Customer Data Incident Response Process and procedures is performed for key areas, such as systems that store sensitive Customer Data. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities and help us better prepare for Customer Data Incidents.

Our processes are tested on a regular basis as part of our certification programs to provide our Customers and Supervisory Authorities with independent verification of our security, privacy, and compliance controls.

SUMMARY

Protecting Customer Data is core to our business. We continually invest in our overall security program, resources, and expertise, which enables our customers to rely on us to respond effectively in the event of a Customer Data Incident, protect Customer Data, and maintain the high reliability that Customers expect.

Our Customer Data Incident Response Progress delivers these key functions:

- A process built upon industry-leading techniques for resolving Customer Data Incidents and refined to operate efficiently at Nebul’s scale.
- Pioneering monitoring systems, data analytics, and machine learning services to proactively detect and contain Customer Data Incidents.
- Dedicated subject matter experts who can respond to any type or size of Customer Data Incident.
- A mature process for promptly notifying affected Customers, aligned with Nebul’s commitments in the Agreement.