Draup

Incident Management Policy

Incident Management and Response Policy

Security incidents are irregular and anomalous conditions that cause — or may lead to — service degradation, loss of critical data, outages, or any form of reduced operational status. These situations require human intervention to avert disruptions or restore the operational status.

This document offers guidance for the staff or incident responders who believe they have discovered or are responding to a security incident.

Reporting a Security Incident

If any staff believes they have discovered or noticed a security incident (as described above), please take the following first steps to report the incident:

1. Please report the incident to your manager as soon as possible.

2. If your manager is not available, please approach the ISO / CEO to report the incident.

The Information security officer (ISO) is responsible for ensuring that reported security incidents are added to the appropriate incident management system where they can be tracked to resolution.

Responding to Security Incidents

It is important to clearly delineate responsibilities during an incident. A quick resolution requires focus and clearly defined responsibilities. Preventing overlaps and ensuring a proper order of operations is vital to mitigation.

At any given point in time, the On-Call-Engineer (OCE) is the first point of contact and is responsible for addressing the incident. Among other things, it is their responsibility to identify the severity of the incident as per the definitions below.

Incident Severity

1. Low severity Incidents are those that do not require immediate remediation. These typically include services of Draup being partially unavailable (for which workarounds exist). These do not require someone to be paged or woken up outside normal working hours.
2. Medium severity incidents are similar to Low severity incidents but could include scenarios like suspicious emails, or unusual activity on a staff laptop. Again, these do not require immediate remediation or triggering of automatic calls outside work hours. Low and medium severity incidents usually cover the large majority of incidents found.
3. High severity incidents are problems where an active security attack has not yet happened but is likely. This includes situations like detection of Backdoors, malware, malicious access of business data (e.g. passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.

4. Critical severity incidents are those where a security attack was successful and something important was lost (or irreparable damage was caused to critical services). Again, in such cases, immediate actions need to be taken to limit the damage.

Internal Communications degraded

If there are IT communication risks (i.e. company phones, laptops, email accounts, etc. are compromised), the team will announce an out-of-band communication tool through any means possible.

Internal Malicious Activity

If you suspect that the malicious actor is a Draup staff member or partner, please contact the ISO or CEO directly. Please do not discuss the issue with other employees.

Incident Response Steps

Once an incident is reported, a staff member or team will be assigned to handle the incident. It is the responsibility of this person or team to decide the severity of the incident. For critical issues, the response team will follow an iterative response process designed to investigate, contain the exploitation, remediate the vulnerability, and write post mortem documents that contain lessons learned.

Further, the following steps will be taken for critical incidents

1. The ISO/CEO will determine if legal counsel should be involved with attorney-client privilege.
2. A staff member or team will be assigned to handle the incident. This person or team will be responsible to limit the damage of the incident, bringing the system(s) back to operational status, and updating the leadership team of the status as required.
3. The team will also create a timeline of all known data related to the incident. The timeline should detail what we know the attacker did at what times.
4. The team should also recommend long term mitigations to avoid a similar crisis in the future.
5. Critical incidents can be followed by a retrospective meeting and a “lessons learned” document.
6. In case of security incidents of specific kinds (like loss of data, data theft), the company leadership will take steps to communicate with the affected customers.

7. In all cases, the company will maintain a record of security, availability, and confidentiality incidents.

Non-Compliance

As stated earlier, our customers depend on us to protect their data. To uphold their trust in us, it is important to have appropriate penalties for any violations of our Incident management and response policy. Draup management will determine how serious an employee’s offense is and decide the appropriate penalty. Penalties may include a warning (oral/written) or suspension or termination for more serious offenses.

Questions

If you have any questions regarding this policy, please reach out to the policy owner.

Incident Management Policy

Version	v1
Created By	Scrut Team, Mar 17, 2025
Approved By	Kashish, Apr 1, 2025
Published By	Kashish, Apr 1, 2025