Mentorloop
4 Regent Street
North Richmond, Vic 3000
Australia

Mentorloop Security Incident Response Plan

In the instance of a security incident taking place at Mentorloop, the goals of this plan are to:

- Verify that an incident has occurred
- Maintain or restore system/business continuity
- Minimise the impact of the incident
- Determine how the incident occurred
- Prevent future occurrences
- Improve security and incident response
- Notify the appropriate stakeholders

Identifying security incidents

We have four basic approaches to identifying potential security incidents:

- Alerts generated by monitoring systems
- Unusual, unexpected, or suspicious events reported by staff or customers.
- Anomalies discovered in audits of system logs
- Vulnerability disclosures

If a staff member discovers or is informed of any of the above, they should contact the technical lead directly and inform management.

A security incident must be investigated if there is reason to believe that any of the following may have occurred:

- Loss of information confidentiality (data theft)
- Compromise of information integrity: loss of, damage to or unauthorised modification of data
- Denial of service or system outages
- Misuse of services including unauthorised access to systems

Investigating potential security incidents

The outcome of the investigation phase is to determine the answer to the following key questions:

- What is the scope and extent of the incident
    - What data has been breached, corrupted or lost?
    - What system components have been compromised?
- Is the incident ongoing or completed?
- What is the business impact of this incident?
    - In the case of an ongoing incident, what will be the impact be if this incident is not prevented
- How did the incident occur?

The technical lead will work with the engineering team to categorise, prioritise and assign a team to respond to the incident.

Category	Description
Critical	Degradation of vital services for many users, serious breaches of network and/or data security, degradation of mission-critical components, risk of damage to public confidence in the business
Major	Degradation of service for a small number of users, disruption of non-essential services.
Minor	Unsuccessful attempts to breach network security, unsuccessful denial of service attempts.

The assigned team will conduct an investigation into the incident by assessing the current state of system components and examining all available system logs.

Responding to an incident

The highest priority in responding to a security incident must be damage containment. This may involve temporary disruption of regular service but the priority must be to minimise the risk of a serious data breach rather than to immediately restore services.

- Any system component that has been compromised should be isolated from the rest of the system; this may involve taking it offline or shutting it down completely.
- Any compromised component should be audited for its use as a possible attack vector for other system components. If it cannot be sufficiently determined that other components have not been breached, they should also be taken offline.

- In the event that any system component must be reprovisioned or rebuilt, evidence pertaining to the incident (system logs, current database or filesystem state, etc) must not be destroyed until forensic investigation into the incident has been completed.
- In the event of a network security breach, all keys and passwords on any components that cannot be confirmed to have not been affected must be rotated.
- Any user accounts that cannot be confirmed to have not been compromised must have their credentials reset.

If there is sufficient reason to believe that customer data has or may have potentially been breached, any affected customers should be contacted directly and notified of the incident. They should be informed of potential risks to their data, the steps being undertaken to mitigate those risks and any options available to them for escalation.

Once the incident has been contained, the team's priority is to identify and eradicate its cause. This may include:

- Patching known vulnerabilities in operating systems and/or applications
- Hardening network security rules
- Implementing and deploying application code changes
- Resetting account credentials for compromised users

System recovery

When the team is satisfied that the damage from the incident has been contained and that the cause or attack vector has been eradicated, regular service of the system must be restored.

- Application instances should be restored, from scratch if necessary.
- Database instances should be restored from backups if necessary.
- All components should be fully patched.
- All intrusion alerts and system logging must be confirmed to be functioning correctly.
- Any temporary constraints implemented during incident response should be lifted.
- All systems must be tested thoroughly before being brought online.

Follow up

Once the system has returned to regular operation, internal stakeholders should be provided with a summary of the incident and how it was responded to. Any technical or policy recommendations from the engineering team to prevent or minimise the risk of further incidents should be presented to management and, if agreed upon, be scheduled for action. Management will decide as to the level of communication that should be made with external stakeholders.

The response to the incident should be reviewed in detail and where necessary policies should be updated. Important questions to ask in review include:

- Could additional procedures or policies have helped prevent the incident
- Were any existing procedures or policies not followed that potentially enabled the incident to take place
- Was the incident response appropriate, timely and effective, and how could it be improved
- Were incident response procedures detailed enough to cover the situation, and if not how can they be improved

Any evidence gathered during the response to the incident should be stored permanently in the event that it needs to be shared with stakeholders, law enforcement, or customers wishing to conduct their own forensic analysis.

In the event of customers wishing to conduct their own investigations into a security incident, Mentorloop will provide support (including access to audit logs) to the extent that it does not breach the Mentorloop Privacy Policy and in accordance with Mentorloop's privacy agreements with its end-users and other customers.

Notifications

Mentorloop will notify affected users and authorities as required by applicable law. Mentorloop will notify affected users and their program coordinators via email within 1 month (or sooner if required by applicable law) of a confirmed security incident. Notifications will include:

- Locations affected by the incident
- How it was discovered
- What personal data was exposed, if any
- How the incident affects Mentorloop customers and community
- What services or assistance, if any, Mentorloop will provide affected users and customers
- What Mentorloop is doing/has done to prevent a similar incident from happening again.

In the event that Mentorloop experiences an outage as a result of a security incident, notifications will also be sent according to the Mentorloop Business Continuity & Disaster Recovery Plan.