Incident Management Policy

A Table of Contents

MENU Technologies AG · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app

A. Context

Protecting personal data and our company assets is a main priority of ours to preserve the trust of our customers & partners and safeguard our intellectual property.

As such, we want to make sure that we can respond to security events in a planned, measured & structured way, to identify, mitigate & resolve the incident as quickly and as safely as possible.

This document describes how security incidents are to be adressed and applies to all MENU personnel.

If you have any questions about this document, please address them to your line manager or information-security@menu.app

B. Terms & Definitions

SIRT (Security Incident Response Team)	Group of MENU team members responsible for responding & managing security incidents, composed of members of the MENU Technology Team, as defined by the *security-incident-response-team* user group in Atlassian. The members of the SIRT are defined by the CTO.
Personal Data	Information related to a Data Subject and that directly or indirectly identifies a Data Subject.
Incident Ticket	A ticket in JIRA Service Desk for the incident that tracks it's progress, documents actions taken & evidence collected and is managed by the SIRT.
System Administrator	Person responsible for managing information infrastructure directly supporting MENU's production application platforms, mostly on AWS. The System Administrator is defined by the CTO.
IT Administrator	Person responsible for managing internal infrastructure & systems, as well as provisioning/deprovisioning internal system accesses. The IT Administrator is defined by the CTO.

C. Policy

- Security incidents should be reported through the appropriate channels (as defined in this document) as soon as possible.
- All MENU team members and external contractors with access to MENU systems are required to report incidents as soon as they are discovered.
- Only the SIRT team is to define if an incident has a security impact or not. MENU team members should hesitate to report an incident, even if they are uncertain of its severity.
- The management of incidents should follow a structured procedure, as defined in this document.
- In the event of a breach, the SIRT is required to inform Data Controllers (customers) and the respective authorities through the means defined in this document.

D. Procedure

This section describes the steps to be taken in managing an incident. All steps after the identification will be performed or coordinated by the SIRT.

1. Identification

In this step, a potential incident is discovered, either internally or by a third-party. Immediately upon discovering or receiving notice of the incident, MENU team members should immediately report it to the SIRT through **internal-incident@menu.app**, which will automatically open a ticket in the *Incident Management* JIRA Service Desk project.

Incidents may be discovered through many ways, including:

- AWS security event alerts
- Automated GSuite alerts to GSuite admins
- Observation of suspicious behaviour
- Support ticket opened by third-party to Technical Operations team
- Customer report to Account Managers or Solution Consultants
- Observation of a non-compliant behaviour, as defined by MENU Policies

Incidents may manifest in many different ways, including:

- (Personal) Data exposed internally or externally to people without the necessary permissions
- Granted system access to unauthorized people
- Breach of physical security environment

Better safe than sorry: If a MENU team member is unsure about if a situation is an incident, they shall still report it to the SIRT, which will decide if an action needs to be taken.

Application bugs shall not be reported as incidents, unless they can lead to a security incident. Bugs should be reported as defined by a separate policy.

The following information should be included in an incident report (via e-mail) to the SIRT:

- Full name and role of the team member reporting the incident
- Date & time when incident was discovered
- Date & time when incident occurred (if known)
- Extensive description of the incident
- Assets affected by the incident
- If this incident relates to any other incident reported previously by the same person

The SIRT is immediately informed of the new incident ticket and the first SIRT member to receive the ticket will assign it to him/herself. The SIRT member should make a decision if the situation needs investigation within 3 hours and if so, proceed with the next step of the procedure. The

SIRT member will involve other SIRT members or other stakeholders in taking the decision, as deemed necessary.
If the SIRT member decides the situation does not need further investigation, they should state the reasoning behind their decision in the ticket and close it.

After reporting an incident, the person that has reported the incident is to remain available and reachable via E-Mail, Phone and Slack for any follow-ups by the SIRT.

2. Analysis

In this step, the SIRT determines if a situation is a security incident. This is done by:

- Analyzing information provided in the initial incident report
- Reviewing logs, including security event logs, access logs, DB logs, audit logs
- Monitoring system metrics, like CPU load, I/O, bandwidth usage, active connections and comparing it with historical data
    - The SIRT may reach out to commercial, product or other teams to identify if anomalies in metrics may be related to marketing campaigns, product releases etc.
- Interviewing team members, not limited to the person that initially reported the incident
- Performing online research

If the situation is identified as a security incident, the SIRT should analyze to determine:

- If the incident has passed or is still ongoing
- The type of security incident
- Impact on MENU or its customers
- System resources or components affected
- If data has been exposed / stolen or destructed
    - The type of data, especially if it affects Personal Data
- If the incident involves malware on any of MENU's systems

The SIRT will categorize the incident into the highest applicable level of one of the following categories:

- Category 1: A threat to public safety or life
- Category 2: A threat to sensitive data
- Category 3: A threat to computer systems
- Category 4: A disruption of services

The SIRT should collect evidence on the incident, for which the following procedure applies:

- Information on the handling of evidence should be tracked, including:
    - Full name and role of the person that collected or handled the evidence
    - Time and date of each evidence handling event
    - Locations where evidence was stored

- If any team member is suspected to be responsible or involved in a security incident, in alignment with the line manager and IT administrator, accesses should be temporarily removed and any physical assets should be confiscated.
- Depending on the incident, physical areas or assets should be secured in their current condition, including:
    - Workplaces
    - Hardware
    - Software

Until decided otherwise by the MENU management team (or defined otherwise in this document), the incident investigation is to be kept confidential and only the stakeholders necessary for the investigation should be involved. It should be communicated to all involved stakeholders that information about the investigation is privileged and should be kept confidential.

Depending on the severity of the incident, the SIRT will request additional resources for the investigation from the MENU management team.

3. Containment

In this step, the SIRT will mitigate the root cause of the security indicident to prevent further damage or exposure. This includes:

- Securing a system component, by shutting it down, disconnecting it from the network or disabling certain functions.
    - This is done in coordination with the system administrator and any other teams responsible for the affected system component.
- If appropriate, backing up the impacted system
- Changing passwords or other authentication/security keys to the affected systems
- Determine if the impacted system should continue operating:
    - If it is safe to continue operating the impacted system, the SIRT will move to the Recovery step
    - If it is not safe to continue operating the impacted system, the SIRT will, in coordination with the system administrator and any other team responsible for the impacted component, cease operations of the component. The SIRT will continue with the Elimination step.

All decisions & actions taken should be documented in the incident ticket, with information on their effectiveness.

If ceasing the operation of a system component leads to a service disruption in MENU's software applications, the system administrator will create an incident in Statuspage for the relevant environment to make sure all stakeholders are adequately informed.

All changes performed need to follow the Emergency procedure of the Change Management Policy.

4. Elimination

In the Elimination step, the SIRT works to remove the vulnerability from the affected component/environment. All attacker's accesses to an environment or all vulnerabilities should be removed at once. The specific steps taken depend on the incident, but the standard process is as follows:

- Eliminate components of the security incident, for example deleting malware or disabling affected user accounts
- Strenghten controls for the affected system component, including:
    - Improving monitoring & logging capabilities, including investigating the possibility of extending existing intrusion detection & prevention systems to automatically identify & mitigate any following similar incident
    - Creating & deploying patches to MENU's internal software in coordination with MENU's development team
    - Consulting external security experts on additional steps that can / should be taken
- Document steps taken & their effectiveness in the incident ticket

Before moving to the next step, the SIRT makes sure to test the new controls and that the elimination steps performed were effective and the incident has been fully resolved.

All changes performed need to follow the Emergency procedure of the Change Management Policy.

5. Recovery

In the Recovery step, the SIRT works to recover the impacted system component in coordination with the system and/or IT administrator. All actions taken in the Recovery step should be aligned with MENU's Disaster Recovery Plan.

The specific actions taken in the Recovery step will depend on the security incident, but may include:

- Installing / deploying patches
- Restoring components from a clean backup
- Re-deploying components from scratch through MENU's CI/CD pipeline

All changes performed need to follow the Emergency procedure of the Change Management Policy.

6. Communication / Notification

If the security incident involved the breach of any customer data, the customer shall be informed through their Account Manager (if available, otherwise directly by the SIRT) within 24 hours of becoming aware that customer data has been breached. The notification to the customer should include:

- Description of the incident, including date & time and affected systems
- The type of data breached, including the amount of data that has been exposed
- Contact information of a person within the SIRT where the customer's security team can obtain additional information & clarify technical details
- Actions taken to patch the vulnerability and prevent the incident from reoccurring

If personal data was breached, the customer should be informed about their obligation to report the breach to the Data Protection Authority of their country within 72 hours. In this case, the following additional information should be included in the notification to the customer:

- If possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- Likely consequences of the personal data breach

The designated point-of-contact in the SIRT should remain available for any inquires from the customer or the Data Protection Authority directly and should work with them to provide any additional information & documentation on the incident.

In the case of an attack, the SIRT should consult with the MENU management team on if the authorities should be informed and/or external forensic investigators should be engaged.

7. Lessons Learned

The SIRT should conduct a post-mortem session to perform the following:

- Create a post-mortem documentation page on Confluence to accompany the incident ticket
- Determine what changes are needed to the information security program and define next steps & responsibilities to implement them
- Communicate all findings & recommendations to MENU's management team
- Review the incident ticket & post-mortem page and make sure it contains all required information (see below)
- Close the incident ticket

It is important that the incident ticket & post-mortem documentation page are complete, as authorities may request access to it as part of their investigation and/or MENU may decide to take legal action against anyone responsible for the attack. The documentation should contain at least:

- Dates & times when incident-related events occurred

- Dates & times when incident-related events were discovered
- Extensive description of the incident, including system components, assets and data that was compromised
- Cause of the security incident and the steps performed to address it, patch the vulnerability and make sure the incident will not reoccur
- Names & roles of all SIRT members involved in the investigation
- Names & roles of all other MENU team members that provided guidance or information during the investigation, including a description of their involvement in the investigation (e.g. what guidance/information was provided)
- All evidence collected by the SIRT together with the evidence handling protocol
- Dates & times when Data Controller and/or authorities were notified