epi European Payments Initiative

INTERNAL, DO NOT SHARE OUTSIDE EPI

Security Incident Procedures

Disclaimer

This document contains internal procedures of EPI. This document is distributed to the members of EPI and internally within EPI. It is Internal and shall be treated according to the provisions established in the EPI policies. The document has been written in present form (“EPI does...) as if described procedures were already live.

Version control

Version	Date	Main changes
0.1	12/08/2023	First draft EPI Incident Management Policy
0.2	19/10/2023	Updated draft specialising to Security Incident Management
0.3	21/06/2024	Update based on now existing general EPI Incident Management Policy. Removing all sections that would duplicate content from the Incident Management Policy.
1.0	02/07/2024	More updates, Rapid 7 inclusion, on-call duty.
1.1	30/08/2024	Update based on alignment regarding on-call duties and lines of support for incidents.

Writing conventions

When reading EPI information security policies, the following writing conventions should be considered:

- the use of "should" and "may" implies that the rule is a recommendation;
- the use of "must", "must not" and "cannot" in a rule implies that the rule must be observed;
- the terms that are capitalised have a specific meaning within this document. The definition of these terms is included in a "*Glossary*" section.
- all clauses included in the policies have the format [XX-YY-00], where "XX" is the identification of this document within the information security policy, "YY" is the specific section and "00" is the number which identifies each clause uniquely.

Table of contents

Version control 3

Writing conventions 3

Table of contents 4

1.0 Introduction 6
- 1.1 Context and purpose of this procedures 6
- 1.2 Definitions 6
- 1.3 Acronyms 6

2.0 Principles and guidelines 6
- 2.1 Guiding principles for Security Incident Procedures 6
- 2.2 Incident Preparation 7

3.0 Roles and contacts related to Security Incidents 7

4.0 Assembly of the Computer Security Incident Response Team 7

5.0 Security Incident– General Process 7
- 5.1 Detection and Identification 7
- *5.1.1 Tooling* *7*
- *5.1.2 External provider* *8*
- *5.1.3 Internal sources* *8*
- *5.1.4 Monitoring and on-call* *8*
- *5.1.5 Analysis and initiation of the Incident Management Procedures* *8*
- 5.2 Containment and Assessment 8
- 5.3 Response and Recovery 9
- 5.4 Communication and notification (Internal and external) 9
- 5.5 Documentation 9
- 5.6 Evaluation and improvements 9

6.0 Response Guides 9
- 6.1 Response guide: Cybersecurity Incidents 10
- *6.1.1 Criteria* *10*
- *6.1.2 Response plan* *10*
- *6.1.3 Incident response team* *10*
- 6.2 Cryptographic Key or Secret Compromise 11
- *6.2.1 Criteria* *11*
- *6.2.2 Response plan* *11*
- *6.2.3 Incident response team* *11*
- 6.3 Information Security Incident (non cyber-security) 12
- *6.3.1 Criteria* *12*
- *6.3.2 Response Plan* *12*
- *6.3.3 Incident Response Team* *12*

7.0 Contact Lists 12

8.0 Related documents 12

9.0 Security Incident Management Documentation Template 13
- Incident Overview 13
- Incident Response Team 13
- Detection and Identification 13
- Containment and Assessment 13
- Response and Recovery 13
- Communication and Notification 13
- Evaluation and Improvements 13
- Incident Closure 13

1.0 Introduction

1.1 Context and purpose of this procedures

The EPI Security Incident Procedures are based on the EPI Incident Management Policy, that provides definition of processes, roles, and responsibilities for handling of Incidents. The Security Incident Procedures describe those procedures that are necessary and used on top of the general Incident Management Policy and Incident Management Procedures to adequately manage Security Incidents.

EPI has prepared these procedures for the **detection of**, **response to and recovery from Security Incidents**. EPI has also taken measures to ensure capabilities and technical support to manage security incidents and in particular cybersecurity incidents. This makes use of various software tools, in particular Atlassian Confluence and JIRA for documentation and communication of topics such as Playbooks, on-call schedules, alerts and analysis of alerts, contact persons in different lines of support and for different scopes. This document collects and refers to these additional operational resources.

The procedures described here naturally focus on

- **Information Security Incidents** without impact on ICT and availability of systems, but with sole impact on confidentiality and integrity of information.
- **Cybersecurity Incidents**, with a malicious threat actor attacking EPI systems.

as other types of incidents (availability of systems and no malicious threat actor) fall within the scope of the Incident Management Policy and Procedures and are adequately handled by them.

The EPI Security Incident Procedure is a live document that aims to be constantly updated as required by updates to the operational procedures, changes to available tooling, new capabilities and most importantly based on experience from actual incidents and incident simulations.

1.2 Definitions

Definitions of the capitalised terms in this document can be found in the "EPI Glossary" and the EPI Incident Management Policy. In the context of these procedures the following definitions are used additionally:

Incident Management Team: The group of people responsible for incident management. In particular, the EPI 1st Line of support, EPI 2nd Line of support, EPI 3rd Line of support, and (Major) Incident escalation Manager as defined in the Incident Management Policy.

Security Event: Any event that could potentially lead to a loss, compromise, corruption or disruption of services, data, or operations. A Security Event is **detected** by automated systems, such as SIEM systems, employees, or external parties.

Security Incident: An undesired and unplanned event which is not part of the standard operation and which causes, or may cause, a loss, an interruption to, the compromise of, the corruption of or a reduction in the quality of a services, data, or operations. A Security Incident is **declared** by the Incident Management or Security Team of EPI after analysis of one or multiple Security Events.

Security Team: The combined team of all Security Experts and Security Engineers from the OSD, PEX and CISO organisation including Heads of Security, Head of Technical Operations and the EPI CISO.

1.3 Acronyms

DNB: Dutch National Bank
CSIRT: Computer Emergency Response Team
EBA: European Banking Authority
NBB: National Belgian Bank
NCA: National Competent Authority

2.0 Principles and guidelines

2.1 Guiding principles for Security Incident Procedures

The implementation of Security Incident Response is guided by fundamental principles that ensure effective security incident handling. The objective of these procedures is to ensure that EPI

- Responds to Security Incidents in a timely and competent manner, to contain the incident and minimize the damage caused by it.
- Creates documentation of Security Incidents and responses, sufficient to understand the Security Incident, its handling and actions resulting from it.

- Communicates information about Security Incidents in a controlled manner. Either using the Incident Management Team and their procedures or independently when information about Security Incidents must be kept confidential.
- Fully resolves and closes Security Incidents and returns to normal operations in a planned and structured way.
- Collects forensic court-type evidence where the Security Incident may be caused by malicious actors.
- Using incidents to improve controls, processes and procedures.

2.2 Incident Preparation

The purpose of the following measures is to assure readiness for incidents, so that in the incident case further measures can be deployed without delay:

- The process to deal with suspected or actual information security incidents has been defined and documented in **Error! Reference source not found.**.
- For common and expectable incidents, procedures to handle them are defined in **Error! Reference source not found.**.

An incident response team has been defined as outlined in

Final date of incident resolution	
Final incident severity and impact ratings	

- . When an information security incident cannot be resolved using established procedures, the IRT should be involved.
- Once a year, incident response must be trained with an exercise.

3.0 Roles and contacts related to Security Incidents

For a complete list of the roles, refer to the general *EPI Incident Policy* document.

4.0 Assembly of the Computer Security Incident Response Team

The standard Incident Management roles are described in the Incident Management Policy. The Security Incident Procedures make use of the same roles. In case of Major Security Incidents, a larger group can be required to handle ICT Security Incidents. In this case the Computer Security Incident Response Team (CSIRT) should be assembled. The team is comprised of

- the (Major) Incident escalation Manager (Head of OSD) as per Incident Management Policy
- the EPI CISO,
- subject matter experts of the EPI 3rd Line of support teams of at least P&E, Security,
- external exports from IT Service Provider, MDR Service Provider, Cybersecurity Insurance Breach Response Service

Additionally, the following members should be included:

- If personal data is involved, the Legal team and the Data Protection Officer need to be included.
- If data or actions of an employee are involved, the HR team needs to be included.
- If wrongdoing or fraud is involved, the Legal team needs to be involved.
- If indications of fraud are present, the Fraud Management team needs to be involved.

5.0 Security Incident– General Process

All Security Incident Procedures involving six separate strands, that need to be executed for every Security Incident. Dedicated Response Guides in the following chapter and operational playbooks at Security Incident Playbooks extends this framework by detailing Response Guides that extend and give guidance for the six strands for different kinds of incidents.

For most Security Incident process of resolution of the Incident is managed by the EPI Incident Management Teams. The involved members of the Security Team oversee and organises execution of all steps defined here. They check that all additional experts that are needed to analyse and solve the incident and to organise communication internally, towards members, and regulatory authorities are involved and convoy the Incident resolution by the Incident Management Teams.

5.1 Detection and Identification

The purpose of the following measures and procedures is assurance of early detection of incidents, so that further measures can be initiated in a timely manner.

5.1.1 Tooling

EPI uses multiple tools for the identification of Security Events:

- **Microsoft Defender** for automated analysis of all Microsoft logs for Security Events, managed by CloudCom.
- **Sentinel One XDR** for automated analysis of additional logs from endpoints, managed by CloudCom.
- **Rapid7 InsightIDR** as SIEM for custom detection rules on all relevant log sources. Managed by Rapid7 with notifications to Security Mailbox and monitoring by security on-call duty.
- **AWS GuardDuty** as specialized SIEM for the AWS environments based on AWS CloudTrail logs. Managed by AWS with notification to Security Mailbox and monitoring by security on-call duty.

5.1.2 External provider

EPI uses external provider to guarantee 24/7 monitoring of Security Events:

- **Rapid7 MDR** (Managed Detection and response) and threat intelligence. Rapid7 MDR monitors the InsightIDR installation for EPI and has a defined procedure for informing EPI Security Team about relevant Security Events and for escalation outside of working hours. Details are maintained at Rapid7 Worfklow Escalation.
- **CloudCom** IT service provider with detection and response capabilities. CloudCom will inform the EPI Security Team using the Security Mailbox and using the "*CC<->EPI Security"* Teams channel, that has been prepared for alerting and direct communication.

5.1.3 Internal sources

Following EPI's Workspace Policy all EPI employees and contractors who become aware of potential Security Incidents are required inform the EPI Security Team via email to security@epicompany.eu. Potential Security Incidents (Security Events) can also include documents that are inadvertently sent to non-authorized parties, access credentials that are made public, lost, or stolen IT devices, malware, or signs of compromised IT systems.

5.1.4 Monitoring and on-call

To ensure that notifications about Security Alerts are received and acted on-call teams with contact data are defined and are constantly updated. Details are maintained at Overview-of-Call-Team-Members---Security as 3rd Line Support Teams in the general Incident Management organization. The on-call schedule is maintained at Overview-On-Call-OSD-Security-SPOC-Responsibility-per-Week.

To ensure that engineering support from the PEX team is available a similar on-call schedule is maintained for PEX at https://epicompany.atlassian.net/wiki/spaces/EP/pages/1496416287/Incident+Management+Policy+On+Call+Duty

The **PagerDuty** tooling and apps are used to ensure availability and reachability of this 3rd Line of support in Engineering. The on-call rotations as well as use of PagerDuty is organized and documented at PEX On-Call-Duty Shift Planning.

5.1.5 Analysis and initiation of the Incident Management Procedures

If the Security Team get notified of a Security Event using the above tools and channels the team analysis the Security Event and documents its analysis in the appropriate medium (Confluence, Jira Ticket, Alert, ..). If a Security Incident is detected the Security Team decides if the general Incident Management Procedures as defined in the *EPI Incident Management Procedures* must be started. This is the case for all Security Incidents that are also ICT Incidents with impact on the availability of EPI services and impact on EPI customers.

To trigger the Incident Management Procedures the Security Team informs the Incident Management Team and always also informs the #monitoring-team-contact Slack channel.

If a Security Incident is a pure Information Security Incidents, that has no impact on the availability of EPI services and impact on EPI customers the Security Team start the Response Guide *"Information Security Incident (non cyber-security)"* described below.

If a Security Incident is a Cybersecurity Incident with likely compromise of EPI ICT systems by threat actors, the Security Team starts the Response Guide "*Cybersecurity Incidents*" described below.

5.2 Containment and Assessment

The responsible Lines of support of the Incident Management Team will assess the situation to determine the scope and severity of the incident. The team will take appropriate steps to contain the incident to prevent further damage. These steps may be outside ordinary EPI operating procedures.

In addition to the actions of the incident management procedures the Security Team determines if any of the Response Guides from the Section below are appropriate for the incident and execute the response guides.

Based on the type of incidents different roles of EPI need to be involved in the Incident response team. After relevant Response Guides are determined, the Security Teams also inform the necessary roles of EPI about the Incident.

As part of the assessment of the Incident Management Procedures the priority of an incident is decided, which also determines if an incident is considered a Major Incident as defined by EBA's Guidelines on major incident reporting under PSD2.

Security Incidents prioritisation follows the criteria defined in the Incident Management Policy and accompanying documents. These criteria are based on the consequences of incidents (Severity / Impact) and are also applicable to Security Incidents.

5.3 Response and Recovery

The responsible Lines of support of the incident management team will implement a response to mitigate the impact of the incident according to the incident management procedures.

For Security Incidents the Security Team supports the implementation of a response and of recovery as subject matter experts. This may involve restoring services, data, or operations that have been disrupted. As a rule, the recovery and stabilisation of services has highest priority during every incident. After successful handling of the incident the Security Team will also work to prevent similar incidents from occurring in the future by performing or participating in a root-cause-analysis and lessons learned meeting.

Measures for response and recovery depend completely on the incident at hand and should be prepared as best as possible. This happens not only in the Response Guides but also by creating and regularly update and review of Security Incident Playbooks. Similarly, by the creation and regular update and review of Runbooks in PEX, e.g., for recovery of services, the import of backups, or taking of forensic evidence.

If the Security Incident is of a unique nature and no applicable Response Guides or Playbooks exist, the Security Team will improvise a response, support the Incident Management team as best as possible, and document steps taken in order to create a Playbook for future, similar incidents.

5.4 Communication and notification (Internal and external)

Incidents need not only be managed but also communicated internally, to members, partners, regulatory authorities and sometimes the public. For all Security Incidents managed as regular Incidents this relies on the procedures of the Incident Management Policy and accompanying documents including Member Support managers.

For Security Incidents the Security Team ensure that the Cybersecurity Insurance Breach Response Service is contacted. The Security Team ensures that for this

Breach Response Service Crisis management network of Zurich is called
via the number **+1 519 340 0140**

For incidents that affect users of the EPI payment system or that are in any other way discussed publicly, additional measures need to be taken to manage public opinion. In these cases, the Security Team supports any spokesperson and the Incident Manger to ensure that accurate and consistent information is being communicated to the press or in social media.

5.5 Documentation

Security Incidents are usually documented as part of the usual incident management procedures. The Security Team additionally documents Security Incidents to include information about its cause, impacts, and response. This uses a restricted directory in SharePoint directory Incidents. In some situation, the documentation of incidents may be classified as EPI Secret, or as EPI Confidential with access by a small group of participants.

In these cases the documentation is (at least until the incident can be communicated more openly) maintained in the restricted SharePoint directory.

5.6 Evaluation and improvements

The actions for handling of Security Incidents are analysed and is used to improve the Security Incident Processes or to create or improve specific playbooks for handling of Security Incidents. For each Security Incident a post-mortem analysis is performed by the Security Team. This can happen in collaboration with Incident Management Team, in particular for Incidents that also are evaluated with postmortem analysis as part of the usual Incident Management Procedures. Any improvements identified are also documented in the incident documentation.

6.0 Response Guides

. Concretisations of the general steps are described below in the form of Response Guides for specific kinds of incidents. These Response Guides include:

Criteria: Criteria to decide if the given type of incident is present.

Response plan: Concrete requirements that are additionally to be executed in this type of incident. Additional requirements can affect individual or many of the general steps that happen during the Incident Management Procedures.

Incident Team: Additional roles that need to be included to the incident response team in this type of incident.

6.1 Response guide: Cybersecurity Incidents

EPI has set in place monitoring tools (SIEM – Security Information and Event Management), that are used to monitor all security-relevant events, and to correlate them. Moreover, EPI ensures that security alerts are assessed timely by the reliance on a Security Operation Centre and 3rd Line of support on-call schedule in the Security Team.

6.1.1 Criteria

A Cybersecurity incident refers to any deliberate attempt to compromise or damage EPI company's systems or infrastructure, such as through unauthorized access, malware, or denial-of-service attacks. Compromised infrastructure refers to any system or component that has been breached or compromised by a cyber-attack.

6.1.2 Response plan

- **Detection and Identification:**
  - Alerts in the EPI SIEM shall be analysed by the Security Operations Centre. The EPI Incident Management Team is informed, and the EPI Incident Management Process is triggered by the Security Team if the SOC's pre-analysis indicates a Cybersecurity Incident. The CISO and CRCO are also informed immediately.
  - The Security Team and IT personnel (in all Lines of support) shall take all necessary steps to preserve forensic evidence (e.g. disk images, VM images, log files) for investigation to determine if any malicious activity has taken place. All such information shall be preserved, and the integrity of forensic evidence shall be protected. The Security Team supports in this.
- **Communication and notification (Internal and external):**
  - For Cybersecurity Incidents the Incident Management Team always also immediately ensure that the CISO, COO, Head of Security and Head of Technical Operations are informed of the Incident.
  - The Cybersecurity Insurance Breach Response Service must be contacted within 72 hours after becoming aware of the Security Event and included in the Incident Management Procedures. The Security Team ensures that for this

Breach Response Service Crisis management network of Zurich is called via the number **+1 519 340 0140**

- **Containment and Assessment:**
  - In the presence of malicious actors, the Incident Management Team shall achieve sufficient certainty that the containment of malicious actors was successful before starting to install new systems for recovery.
  - Containment and assessment for Cybersecurity Incidents shall be based on Security Incident Playbooks provided by the Security Team. The Security Team supports the Incident Management Teams in the necessary and defined steps.
  - If production ICT systems of EPI company, either of the corporate IT or of the production systems of the payment platform, are compromised, these incidents must be classified at least as P2 – High Incidents.
  - If the assessment makes it like that threat actors have ongoing access to EPI employee accounts, access to Confidential or Secret EPI information, or the production payment systems then an Incident must be classified as P1 – Critical.
- **Response and Recovery:**
  - Response and recovery for Cybersecurity Incidents shall be based on Security Incident Playbooks provided by the Security Team. The Security Team supports in all steps necessary and continuously improves Playbooks for this purpose.
- **Documentation:**
  - Documentation of Cybersecurity incidents shall include an analysis of the root cause, complete documentation of the evidence collected, and a log of the measures for containment, mitigations and recovery applied (e.g. patching of system, re-installation from known-good images, separation of systems on a networking level, termination of logged-in sessions).
- **Evaluation and improvements:**
  - Following a Cybersecurity Incident a post-mortem analysis shall be conducted by the CISO, the Security team and relevant members of the involved teams. The post-mortem shall include an analysis of the root cause of the incident and lessons learned.
  - Playbooks of the Security team shall be updated based on the lessons learned.
  - A post-mortem also shall be conducted in case the incident proves to be a near miss. In this case post-mortem and lessons learned shall focus on measure to prevention of similar issues in the future.

6.1.3 Incident response team

The Incident Management Team ensures that at least one member of the Security Team and the CISO are always included in the Incident Management. If IT systems of a service provider are potentially involved at least one security expert of the service provider shall be included in the incident response team. If IT systems of the payment systems are potentially involved at least one 3rd Line of support engineer of PEX shall be included.

6.2 Cryptographic Key or Secret Compromise

6.2.1 Criteria

Cryptographic Key or Secret Compromise refers to any authentication data or cryptographic keys that have been exposed to, accessed by or stolen by unauthorized (third) parties. This includes, but is not limited to, login credentials, passwords, encryption keys, access tokens and other access codes. The criteria as satisfied also in Incidents that involve threat actors that makes use of keys or credentials that should not be available to them.

6.2.2 Response plan

- **Containment and Assessment:** The Security Team must assess how the compromise of keys or secrets happened. This assessment is of utmost importance to ensure that no other keys or secrets are compromised, and that keys or secrets are not re-compromised after being exchanged. The Security Team must make the state of their assessment available to the Incident Management Teams so that actions can be based on the latest information.
- **Response and Recovery**: The Security Team must ensure that a reset of involved passwords is performed, access privileges are revoked, and other measures are taken to prevent further unauthorized access as soon as possible. This should also include keys and credentials that could also be compromised given the current state of analysis. Additional logging on use of the compromised secrets must be implemented, if possible, ideally using monitoring of existing logs.
- **Reporting and Documentation**: If the compromised keys or secrets affects EPI customers, partners, or other stakeholders, they need to be notified as soon as possible. The Scheme, Marketing and PR teams need to be involved to handle reporting. The notification should include information about the nature of the compromise, the steps EPI is taking to address it, and any actions affected parties should take to protect their systems and regain access after revocation of keys and accounts during the Response actions.

6.2.3 Incident response team

The incident response team shall always include at least a member of the 3rd Line of support Security Team. If cryptographic keys are compromised, the incident response team shall contain a member from the OSD Key Management Office (KMO) and an Engineer from the Product and Engineering team working with the KMO for HSM activities.

6.3 Information Security Incident (non cyber-security)

6.3.1 Criteria

A non-digital information asset of EPI has been lost or compromised, such as physical documents, a hardware device, or verbal communication.

6.3.2 Response Plan

If the information asset has been lost, it shall be established whether the asset is destroyed or should be treated as potentially in the hands of unauthorised persons (thieves or finders). In the latter case it shall further be established if the information is readily accessible to unauthorized persons (e.g. a paper document) or can be assumed to be safe from all but highly competent attackers (e.g. an encrypted hard drive). In the case of hardware devices, remote wiping options shall be deployed in either case.

Lost information shall be restored from backups or physical copies where possible. Where not possible, steps to replicate or replace the lost information, depending on its importance, shall be evaluated.

If the information asset has been compromised, an assessment of the possible impact given what is known about the attacker must be made and containment steps identified (e.g. if the threat is that the information could be leaked to the public, going public first may be the best option). Possibly affected parties, both within and outside of EPI, shall be notified as appropriate.

Possible legal steps to protect EPI's interests, such as options to suppress publication of the compromised information, shall be evaluated with the legal team.

6.3.3 Incident Response Team

The incident response team shall always include the CISO and should usually include the legal team as in most cases theft or unauthorized interception of telecommunications are involved.

7.0 Contact Lists

In all Incidents customers and members can be affected. The Security Team makes use of the existing contact lists of the Incident Management Team at Member Banks Operational Contacts.

The Security Team started work (in the Security MAG Subgroup) to add specific security contacts to this list to reduced indirection in case of specific security related questions and incidents.

8.0 Related documents

The following documents, standards and guidelines are related to this policy:

- EPI Incident Management Policy 1.1
- EPI Incident Management Procedures 1.1
- EPI IT Crisis Management Procedures 1.1
- EPI Fraud Incident Procedures 1.1
- EPI Problem Management Policy 1.1

9.0 Security Incident Management Documentation Template

Incident Overview

Incident ID	NNN/YYYY
Date and Time of start of incident	
Short description	
Type of Incident (e.g., security breach, fraud, operational failure) and impact	
Major Incident under PSD2?	Yes / No

Incident Response Team

Incident response team members involved:	

Detection and Identification

Indicators of how and by whom the incident detected?	
How was the Incident Team informed?	

Containment and Assessment

What response actions was taken for (initial) containment?	
Assessment of the situation	

Response and Recovery

What response actions have been taken (e.g. eradication, recovery)?	
What remediation actions have been taken (e.g. patching, system upgrades)?	
What recovery actions have been taken (e.g. data restoration, system reconfiguration)?	
When have these actions been taken (timeline/timeframes)?	

Communication and Notification

Which internal and external stakeholders have been notified, when, and by whom?	Stakeholder / yyyy-mm-dd / by X …
Which communications plans and procedures have been followed?	
Details of external communication (e.g. who else was notified, when)	

Evaluation and Improvements

Evidence collected and analyzed	
Root cause analysis results	
Lessons learned from the incident	
Recommendations for improving incident management procedures	
Plan for implementing recommended improvements	

Incident Closure

Final date of incident resolution	
Final incident severity and impact ratings	

European Payments Initiative

Security Incident Procedures– August 30th, 2024 – V1.1