CENTRE FOR CYBERSECURITY BELGIUM

FIRST AID IN THE EVENT OF A CYBER INCIDENT

ESSENTIAL READINESS AND INCIDENT RESPONSE

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: May 2026
Version: 1.0 English
Author: The Centre for Cybersecurity Belgium (CCB)

The Centre for Cybersecurity Belgium (CCB) is the national authority for cybersecurity in Belgium. The CCB was established by Royal Decree of 10 October 2014. Based on its legal mission, the CCB informs and advises organisations on improving readiness and incident response.

Table of contents

Introduction

This document summarises the essential capabilities and actions organisations should have in place to ensure effective incident handling and coordination with the CCB.

It also complements the CyberFundamentals Framework and the Safeonweb@work guidance by focusing on operational essentials.

1. Before an incident: minimum readiness capabilities

Organisations should have at least the following basic technical capabilities to quickly detect, contain and recover from a cyber incident:

Early warning and rapid response

- Someone (internal or external) must monitor for suspicious activity 24/7 and be able to take immediate action (Security Operations Centre).

Protection of laptops and computers

- All devices should have security software that can automatically detect and block harmful activity (Endpoint Detection and Response).

Visibility over network activity

- Key systems should centralise activity logs so issues can be identified quickly (Security Information and Event Management).

At minimum this should include:

  - user accounts and login systems
  - firewalls and remote access
  - device protection
  - email security
  - key servers and applications

This information should be kept for at least 90 days (longer is recommended for critical systems).

Strong authentication controls

- Multi-Factor Authentication (MFA) must be enabled for all users, especially administrators and remote workers.

Limiting attacker movement (network segmentation)

- The network should be designed so that if an attacker breaks into one system, they cannot easily move to others.

Reliable backups

- Organisations need a backup strategy that includes:

  - at least one copy that cannot be changed or deleted (immutable)
  - regular testing to make sure restoring data works

Alternative communication channel

- Organisations should maintain alternative communication channels independent of corporate systems, in case these systems are unavailable or compromised.

Accurate inventory of assets

- Maintain an up-to-date inventory of:
  - all devices and systems
  - how the network is structured
  - important IP addresses

Emergency ('break-glass') access accounts

- Maintain special emergency accounts and procedures for situations where the normal login system is down.

Offline emergency information

- Critical information should also exist on paper, such as:
  - step-by-step guides (playbooks)
  - key contacts
  - escalation paths
  - vendor support hotlines
  - response procedures for ransomware incidents, data breaches, fraudulent emails, or DDoS attacks

Incident tracking

- Use a simple tool or system to record:
  - what happened
  - actions and decisions taken
  - affected systems
  - evidence and indicators found

These measures represent **the minimum technical baseline** to detect a cyberattack early, limit the damage, and recover effectively.

1.1. ORGANISATIONAL

Technical measures alone are insufficient. Good governance and clear preparation are just as important, and fully aligned with NIS2 requirements.

Organisations should have at least the following:

A clear incident plan

- A simple Incident Response Plan that explains who does what, and how issues are escalated.

Plans to keep the business running

- A Business Continuity Plan describing how critical activities will continue during a crisis.
- A Disaster Recovery Plan that sets priorities and defines how quickly systems must be restored.

A crisis communication approach

- A clear plan for **managing communication during a crisis**, both internally and externally.

A 24/7 contact list

- An up-to-date list of key contacts, including:
  - technical teams
  - leadership
  - legal advisors
  - communications
  - external partners

A simple risk management approach

- A defined way to identify, evaluate, and manage risks. Even a lightweight framework is sufficient.

Regular exercises

- Tabletop exercises for both technical teams and executives, so everyone knows what to do when an incident happens.

For the full baseline governance model, see the CyFun® and Safeonweb@work resources.

2. During an incident: first 24 hours

The first 24 hours of an incident are **crucial**.

Priorities are:

- Contain the incident,
- Preserve evidence, and
- Coordinate early with the right people.

The following outlines the essential actions of what needs to happen.

2.1. IMMEDIATELY (T+0)

As soon as you suspect an incident:

1. Activate your Incident Response Plan

Everyone should know their role and what to do next.

2. Switch to an alternative communication channel

Use a communication method outside your normal company systems (e.g. Signal, Threema, SMS) in case email or chat is compromised.

3. Preserve evidence

Keep logs and system information intact. This helps understand what happened and supports recovery and investigation.

4. Do NOT wipe, reinstall, or reboot systems

Only do this if absolutely necessary, and after evidence is secured. These actions can destroy critical information.

5. Document everything

Document:

- what you did
- when you did it
- what you observed

This supports **coordination, investigation, and reporting**.

2.2. WITHIN THE FIRST 24 HOURS

Notify the CCB early

If you suspect a significant incident, inform the CCB even if you do not yet have all the details.

Early notification allows:

- faster support
- improved situational awareness
- coordinated response across sectors

Share the basic information you have:

Provide what is available at that moment:

- Whether the incident appears malicious
- Known or estimated impact
- Systems or services affected
- Actions already taken

Where to notify:

- Call when urgent – the reporting form may be completed afterwards
    - Emergency contact CCB: +32 2 501 05 60
- Online reporting: https://notif.safeonweb.be/
- File a complaint with the police
- Notify your cybersecurity insurance company (where applicable)

Why this matters: Early notification and good documentation help contain the incident more quickly and ensure support can be mobilised quickly.

3. During an incident: within 72 hours

Within the **first 72 hours**, organisations should have established a clearer understanding.

Key actions:

Submit a formal notification (if applicable):

- If the incident meets **NIS2 thresholds**, send the official notification.

Share updated information:

Provide whatever is known at this stage, including:

- the **scope** of the incident
- the **impact** on systems or services
- any **indicators of compromise (IOCs)** found
- measures already taken to **contain** the incident
- business impact and operational effects

If personal data has been compromised:

- Notify the Data Protection Authority (DPA) as required under GDPR.

Keep the CCB updated:

- Continue sharing updates with the CCB as new information becomes available.

Why this matters: Clear reporting and transparency early in the process make coordination easier and reduce broader risks.

4. During an incident: within 1 month

Within one month after the initial notification (or after the incident is resolved), a final assessment should be prepared.

Prepare a final report:

The report should include:

- a root cause analysis (how the incident started)
- a timeline of what happened
- the full impact assessment
- all containment and eradication actions
- recovery steps taken
- long-term remediation measures
- clear lessons learned

Ongoing incidents:

If the incident is still active after one month:

- provide a progress update
- submit the final report within one month after the incident is closed

Why this matters:
Post-incident reviews strengthen organisational resilience and prevents recurrence.

5. Lessons learned and continuous improvement

Run regular exercises:

- Hold tabletop exercises at least once a year, and after major changes.
- Run targeted technical tests such as:
  - backup restore tests
  - network segmentation and isolation drills
  - identity recovery drills

Use a structured after-action process:

- Have a formal **after-action review**
- Track remediation measures through to completion

This fits evidence-based improvement and continuous readiness.

6. Operational co-ordination with the CCB

To work effectively with CCB during a crisis, organisations should ensure:

A clear 24/7 contact structure

- A permanently reachable contact point
- Clear escalation path: incident manager, CIO, CISO, communications, DPO

Clear thresholds for notifying the CCB

- Notify the CCB when a significant incident is suspected, even if information is still incomplete.

Proper evidence handling

- Preserve logs and artifacts
- Avoid wiping, reinstalling, or rebooting systems before triage
- Document actions and timestamps

Information package ready to share

Have these elements ready for coordinated response:

- affected services
- scope
- IOCs
- timeline
- mitigation actions
- business impact

Agreed secure communication channels

- Zoom for coordination meetings
- Signal/Threema/phone for crisis communication
- Encrypted exchange for sensitive documents

7. How the CCB fits into an organisation's playbooks

Triage and qualification

- Contact the CCB when a significant incident is suspected or when guidance or new IOCs are needed.

Forensic insight

- The CCB helps analyse evidence, understand the entry point, and identify the root cause.

Containment and eradication

- Share IOCs and TTPs
- Receive guidance on mitigation measures
- Participate in coordinated response if part of a larger campaign

Notification

- Use https://notif.safeonweb.be/
- Provide mandatory fields
- Provide the CCB with regular updates as the situation evolves

Post-incident

- Deliver the final report
- Apply recommendations for improvement

This is fully aligned with the approach of **collaboration, preparedness, and sector-wide resilience**.

Annex 1: useful links

CyberFundamentals Framework: https://cyfun.eu

NIS2 Notification Guide: https://ccb.belgium.be/sites/default/files/2025-08/NIS2_Notification_guide_v1.3-EN.pdf

CCB first point of contact: https://ccb.belgium.be/cert/first-port-call-event-cyberattack

Notification of an incident form: https://notif.safeonweb.be/

Crisis communication in the event of a cyberattack: https://atwork.safeonweb.be/news/crisis-communication-event-cyber-attack

Safeonweb at work: https://atwork.safeonweb.be/

Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

This document contains technical information written mainly in English. Indeed, this technical information is taken directly from reports communicated to the CCB by various international partners (European network of CSIRTs, international organisations, foreign companies, etc.), which are written in English. Moreover, this information related to the security of networks and information systems is addressed to the organisations concerned under the benefit of urgency and to IT services which use the English terms of computer language.

A translation into Dutch, French or German of this technical information can nevertheless be requested from the CCB.

The CCB accepts no responsibility for the content of this document.

The information provided:

• is exclusive of a general nature and does not take into account every specific situation;

• is not necessarily exhaustive, precise or up to date in all respects.

Responsible editor:

Centre for Cybersecurity Belgium
Mr. De Bruycker, General Director
Rue de la Loi, 1
1000 Brussels

Legal Deposit: D/2026/14828/007