CENTRE FOR
CYBERSECURITY
BELGIUM

NATIONAL CSIRT CHARTER

2026

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: January 2026
Version: 2.0 English
Author: Centre for Cybersecurity Belgium (CCB)

The Centre for Cybersecurity Belgium (CCB) is the national cybersecurity authority and national CSIRT in Belgium. The CCB supervises, coordinates and oversees the implementation of Belgium's cybersecurity strategy. Through optimal information sharing, companies, the government, NIS2 entities and the public can ensure they have appropriate protection. The Centre for Cybersecurity Belgium (CCB) was established by the Royal Decree of 10 October 2014.

Table of contents

Introduction

The Centre for Cybersecurity Belgium (CCB) is the national cybersecurity authority in Belgium. The CCB acts as the national Computer Security Incident Response Team (CSIRT). The operations of the national CSIRT as a public service are set out in a legal framework, supplemented by decisions of the Council of Ministers and internal documents. This charter compiles the essential elements from these different sources into one accessible document.

While modifying a charter often is not advisable, this is not a static document. The charter can be modified depending on the legal or budgetary context, or simply after internal research on its relevance. In principle, the document is re-evaluated every year.

1. General information

The Centre for Cybersecurity Belgium (CCB) was established through the Royal Decree of 10 October 2014.

The CCB has been designated as the national cybersecurity authority under the implementation[1] of the NIS2 Law[2]. In this role, the CCB supervises, coordinates and oversees the application of the Belgian cyber security strategy in particular, as well as compliance with the NIS2 Law by the entities involved. Through optimal information sharing, companies, the government, NIS2 entities[3] and the public can ensure they have appropriate protection.

The main missions of the CCB as the national cybersecurity authority[4] are the following:

- monitoring, coordinating and overseeing the implementation of the relevant Belgian policy;
- from an integrated and centralised approach, managing the various cybersecurity projects;
- ensuring coordination between relevant services and authorities, and public authorities and the private or scientific sector;
- formulating proposals to adapt the regulatory framework in the field of cybersecurity;
- in cooperation with the Coordination and Crisis Centre of the government, ensure crisis management in the event of cyber incidents;
- drawing up, disseminating and overseeing the implementation of standards, guidelines and security standards for the various information systems of administrations and public institutions;
- coordinating Belgian representation in international cybersecurity forums, following up international obligations and proposals of the national position in this area;
- coordinating the evaluation and certification of the security of information and communication systems;
- informing and raising awareness among users of information and communication systems.

Under the NIS2 Law, the CCB also acts as the national CSIRT[5]. The Cyber Emergency Response Team (CERT) and the Cyber Threat Research & Intelligence Sharing (CyTRIS) team are the two operational services that together form the national CSIRT within the CCB.

The remit of the CERT is to analyse, contain, mitigate and stop cyber-attacks within Belgium. The CERT provides technical expertise and assistance to other public services. Certain services are provided proactively, but most of the work of the CERT is similar to that of a "cyber fire department."

CyTRIS is responsible for the initial contact with organisations that report an incident to the CCB. This service of the CCB monitors various sources on a daily basis, collects and organises information that may be useful in warning potential victims, conducts in-depth CTI analyses and produces strategic reports. CyTRIS also sends spear warnings (individual messages) to organisations where a given vulnerability has been identified on IT infrastructure, malware has been discovered, or stolen login credentials have been found. In addition, CyTRIS organises regular online and physical events to inform stakeholders about active cyber threats and how to protect against them.

The main missions of the CCB as the CSIRT[6] are the following:

- monitoring and analysing cyberthreats, vulnerabilities and incidents at the national level;
- providing early warnings, notifications and announcements and disseminating information to affected essential and important entities and to competent authorities and other relevant stakeholders regarding cyber threats, vulnerabilities and incidents, in near-real time if possible;
- responding to incidents and providing assistance to affected essential and important entities;
- collecting and analysing forensic data and providing dynamic risk and incident analysis and situational

[1] Royal Decree of 9 June 2024 implementing the Law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security, art. 3.
[2] Law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security (NIS2 Law) The NIS2 Law is the transposition of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (the "NIS2 Directive") in Belgium.
[3] Essential and important entities covered by the scope of the NIS2 Law.
[4] NIS2 Law, art. 17.
[5] NIS2 Law, art. 15-16.
[6] NIS2 Law, art. 19.

awareness related to cybersecurity;
- participating in the CSIRT network,
- acting as coordinator for the coordinated disclosure of vulnerabilities process;
- contributing to the rollout of secure instruments for information sharing;
- proactively and non-intrusively scanning publicly accessible network and information systems
- detecting, observing and analysing computer security problems;
- cooperating and, where appropriate, exchanging relevant information.

"Cybersecurity" refers to all measures that ensure the confidentiality, availability and integrity of information and communication technologies (ICT): technical measures, as well as awareness-raising actions for users.

However, cybersecurity is not about using ICT simply as a tool for activism, terrorism, espionage, subversion or generally criminal activities. These acts fall under the jurisdiction of services other than the national CSIRT (police, State Security, etc.). Identifying the perpetrators of crimes does not fall under the competence of the national CSIRT either.

However, any risk, breach of confidentiality, integrity and availability of ICT systems, for any reason, is a cybersecurity issue.

2. Target audience

The target audience is all the parties who can use the services of the national CSIRT. Certain services are only available to part of the target audience.

Unless there is an explicit legal provision, being part of the target audience of the national CSIRT does not impose any obligation on the relevant companies or organisations vis-à-vis the national CSIRT, but it means that the national CSIRT makes its services available to these companies or organisations.

Who can rely on the national CSIRT?

- Essential entities under the NIS2 Law.
- Administrative authorities: the ICT infrastructure of Belgian public administrations.
- Other important entities as defined in the NIS2 Law may also request assistance, but this will be provided on a best-effort basis and to a more limited extent.
- The general public only has access to a limited part of the services of the national CSIRT.
- Private legal entities that do not fall under NIS2 can rely on a limited part of the services of the national CSIRT.
- Computers, networks or communication systems that are classified within the meaning of the Law of 11 December 1998 on classification and security clearances, security certificates and security advisories fall under the jurisdiction of the National Security Authority (NSA) and are therefore outside the scope of the CCB and the national CSIRT.

3. Competence

The national CSIRT plays a coordinating and advisory role. Article 21 of the NIS2 Law states that the national CSIRT shall take all appropriate measures to achieve its remit and fulfil its obligations. These measures must be proportionate to the objectives, and consistent with the principles of objectivity, transparency and non-discrimination.

In this context, without prejudice to the Code of Criminal Procedure[7], the national CSIRT may possess, disclose or disseminate any available data, or make any use of it, even if this data originates from unauthorised access to an information system by a third party.

The national CSIRT always fulfils its missions with the caution expected of a governmental authority, always ensuring as a priority that the functioning of the ICT system is not disrupted and taking all reasonable precautions to prevent material damage thereto.

[7] Art. 28quinquies, § 1, and 57, § 1.

4. Services

There are a broad range of services that can be proposed by a national CSIRT. These depend both on the target audience and the CSIRT's authority over it, as well as its institutional position. National CSIRT services are generally classified into three categories: proactive services, reactive services and services for managing security quality. This classification is reprised in this chapter, and the service offering of the national CSIRT is described.

4.1. PROACTIVE SERVICES

Proactive services are targeted at improving the security infrastructure and processes of the target audience before an incident occurs or is discovered.

MONITORING AND ANALYSIS OF CYBER THREATS, VULNERABILITIES AND INCIDENTS

The national CSIRT's remit is to detect, monitor and analyse online cyberthreats, vulnerabilities and incidents at national level. On a daily basis, a team within the national CSIRT monitors the threat landscape to identify relevant cyberthreats and vulnerabilities in good time. Additionally, the national CSIRT provides strategic, operational and tactical CTI reports to further analyse specific threats.

INFORMATION SHARING

The national CSIRT provides early warnings, notifications and announcements regarding identified vulnerabilities and cyberthreats through its website, social media, the Early Warning System (EWS)[8] and, when necessary, through direct contact (spear warnings[9]) to alert relevant stakeholders of the risks entailed by new vulnerabilities or threat vectors. In addition, it organises regular online and physical events to inform target audiences about active cyber threats and how to protect against them.

MONITORING THE CYBER DOMAIN

The national CSIRT continuously monitors technology trends, developments and solutions in the domain of cybersecurity and by extension, information security in its broadest sense. This monitoring provides input for others and makes it possible to stay abreast of the latest developments in the field.

DETECTION, OBSERVATION AND ANALYSIS OF SECURITY PROBLEMS

The remit of the national CSIRT is to detect, observe and analyse online security problems. It is therefore the central point of contact for notifications of security incidents and information about cyberthreats[10].

SECURITY ASSESSMENTS / PENETRATION TESTS / ATTACK SURFACE MANAGEMENT

Upon request, and subject to the availability of resources, the national CSIRT may conduct an assessment or penetration test of the infrastructure (or part of it) of its target group, to identify vulnerabilities with potentially significant impact. In addition, it can proactively assess risk from the perspective of an attacker by detecting Internet-facing vulnerabilities to reduce the number of possible access points within target groups to the network. It is possible that the national CSIRT has to work with (external) third parties to provide this service.

[8] See https://ccb.belgium.be/cytris/early-warning-system.
[9] See https://ccb.belgium.be/cytris/faq-on-spear-warnings.
[10] See https://ccb.belgium.be/cert/report-incident.

DISSEMINATION OF CYBERSECURITY INFORMATION

Where appropriate, the national CSIRT publishes guidance or links to similar documents, which may be of interest to the target audience[11].

DETECTING AND INFORMING ABOUT VULNERABLE OR INSECURE SYSTEMS

If it does not adversely affect the operations of the services of the entities, the national CSIRT may proactively and non-intrusively scan publicly accessible network and information systems to detect vulnerable or insecurely configured network and information systems, and notify the affected entities.

4.2. REACTIVE SERVICES

The reactive services are intended to respond to requests for assistance, alerts, and in general any threat or attack directed at the systems of the target audience of the national CSIRT.

INCIDENT HANDLING

- First contact and registration in the event of (NIS2) incidents

Processing (incident) notifications via telephone and e-mail, as well as making initial contact if necessary.

- Incident analysis

At the request of the target audience, the national CSIRT conducts a postmortem analysis of a cybersecurity incident. The aim of this analysis is to ascertain the extent of the incident and the damage inflicted, identify the root cause and make recommendations, if necessary.

- On-site incident management

At the request of certain members of its target audience, the national CSIRT will send specialists to assist local teams in managing a specific incident.

- Support with incident management

The national CSIRT provides support to its target audience in handling security incidents. This support may include advice by email or phone, assistance with forensic data analysis, etc.

- Coordination of incidents

The national CSIRT coordinates the response to incidents, in cooperation with relevant actors. In the event of serious incidents, the national cyber emergency plan may be activated.

VULNERABILITY MANAGEMENT - RESPONSE COORDINATION

When a vulnerability is identified in a given software product, the national CSIRT can coordinate mitigation and communication efforts between the various parties involved (researcher, software provider, users, etc.) upon request[12]. It may be necessary for the national CSIRT to collaborate with third parties in order to provide this service.

ARTEFACT ANALYSIS

An artefact is what remains after an (attempted) intrusion into an ICT system. Files, logs, or information systems

[11] See https://ccb.belgium.be/advisories
[12] See https://ccb.belgium.be/regulation/cvdp

are (non-exhaustive) examples of artefacts. The national CSIRT may analyse any artefacts that are reported. It is possible that the national CSIRT has to work with third parties to provide this service.

4.3. SERVICES IN THE AREA OF SAFETY QUALITY MANAGEMENT

These services make use of the findings and lessons learned from the work of the various reactive services.

AWARENESS-RAISING

The national CSIRT is involved in the awareness campaigns of the CCB. In addition, it organises regular online and physical events to inform target audiences about active cyber threats and how to protect against them.

TRAINING

The national CSIRT has the possibility to develop training in the areas within its competence and to organise training sessions. It may be necessary for the national CSIRT to collaborate with third parties in order to provide this service.

4.4. SERVICES NOT PROVIDED BY THE NATIONAL CSIRT

Proactive services:

- General risk analysis and modelling
- Business continuity planning (BCP/DRP) and Security advice
- Evaluation or certification of security products

Reactive services:

- Vulnerability management - patching vulnerabilities (corrections)
- Operational security
- Reconstruction in the event of a cyber attack

5. Service level

The national CSIRT can be contacted by e-mail or telephone[13] during office hours (9:30 a.m. to 4:30 p.m.) Monday to Friday, outside official closing days.

Acknowledgement of receipt of emails sent to the national CSIRT are automatically sent within minutes. This automatic system assigns a unique number to each notification. It is not stated that the CSIRT will be able to systematically respond to the mail; this depends on the severity of the incident and the quality of the correspondent.

In cooperation with the National Crisis Centre (NCCN) of the Ministry of Interior, the national CSIRT is available by phone around the clock to handle serious incidents for essential NIS2 entities.

[13] For contact details, see Section 6.

6. Summary of the policy of the national CSIRT

6.1. TYPES OF INCIDENTS AND LEVEL OF SUPPORT

The national CSIRT handles any incident related to a network or information system located on Belgian territory, or any Internet domain ending in ".be". The level of support depends on the severity of the incident and the quality of the correspondent.

Priority to the target audience is given as follows:

1. Essential entities under the NIS2 Law.
2. Administrative authorities: the ICT infrastructure of Belgian public administrations.
3. Important entities as defined in the NIS2 Law may also request assistance, but this will be provided on a best-effort basis and to a more limited extent.
4. The general public only has access to a limited part of the services of the national CSIRT. Private legal entities that do not fall under NIS2 can rely on a limited part of the services of the national CSIRT.

Computers, networks or communication systems that are classified within the meaning of the Law of 11 December 1998 on classification and security clearances, security certificates and security advisories fall under the jurisdiction of the National Security Authority (NSA) and are therefore outside the scope of the CCB and the national CSIRT.

6.2. COLLABORATION, INTERACTION AND INFORMATION DISSEMINATION

The national CSIRT handles the information it receives in accordance with the applicable Belgian legislation. The national CSIRT therefore pays significant attention to protecting the personal and sensitive information it receives.

As stated in the national cyber emergency plan[14], the national CSIRT coordinates the activities of the various stakeholders in the event of a national cybersecurity incident. In the event of a national cybersecurity crisis, the national CSIRT works together with the National Crisis Centre (NCCN) to coordinate the activities of the various stakeholders[15].

If it is necessary to communicate personal information to handle an incident, the national CSIRT will be careful to only send the minimum required information.

Data transmitted via e-mail in encrypted form will only be stored in this form and will only be decrypted if necessary for resolving an incident. If it becomes necessary to transfer this data, this will also be encrypted.

The national CSIRT uses and respects the Traffic Light Protocol 2.0 as described by FIRST[16].

The national CSIRT will share its experience with its peers and its target audience to the extent possible, provided this does not violate the above-stated provisions. Specific attention will be paid to the following groups: EGC6, TF-CSIRT7, FIRST8, and the EU CSIRTs Network.

Only persons specifically designated by the CCB will have contact with the press.

[14] The National Plan for Cybersecurity Incidents and Cyber Crisis Response (National Cyber Emergency Plan for short). This plan is a national plan within the meaning of Article 9, § 2, of the Law of 15 May 2007 on Civil Security. This plan is drawn up by the CCB together with the NCCN. The national cyber emergency plan is not a public document. See also art. 29 of the NIS2 Law.
[15] NIS2 Law, art. 18.
[16] https://www.first.org/tlp/

6.3 COMMUNICATION AND AUTHENTICATION

The national CSIRT can be contacted by e-mail at: info@ccb.belgium.be. The national CSIRT can also be reached by phone at +32 (0)2 501 05 60 exclusively in cases of urgent assistance in the event of incidents. The national CSIRT is available during office hours (9:30 a.m. to 4:30 p.m.) from Monday to Friday, outside official closing days.

For the handling of serious incidents affecting essential NIS2 entities, the national CSIRT is available by phone around the clock in collaboration with the National Crisis Centre (NCCN) of the Ministry of Interior.

PGP encryption may be used to ensure secure and discrete communications. Up-to-date information on available email addresses with their PGP keys are listed at: https://ccb.belgium.be/cert/send-encrypted-message.

The national CSIRT has staff members authorised to handle classified information within the meaning of the Law of 11 December 1998 on classification and security clearances, security certificates and public regulated service.