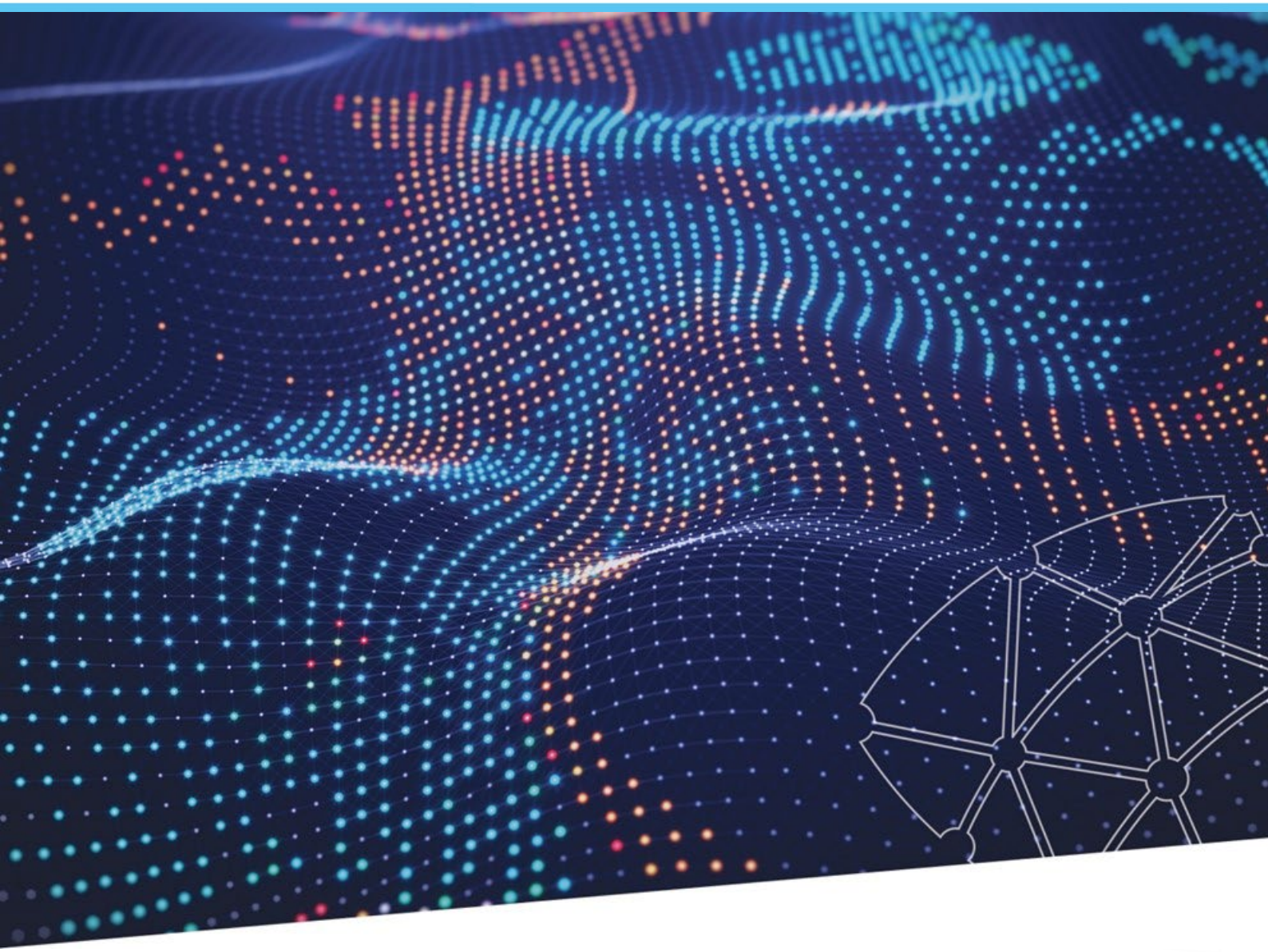
CENTRE FOR
CYBERSECURITY
BELGIUM



NIS2 NOTIFICATION GUIDE

Version 08.2025 – 1.3

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Introduction

The law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (the "NIS2 law") transposes Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (the "NIS2 directive").

In order to address the expanding cyber-threat landscape and the emergence of new challenges, the European Union has adopted new legislation on measures to ensure a common high level of cyber security across the Union (Directive 2022/2555 of 14 December 2022 - the so-called "NIS2 directive"), which replaces the "NIS1 Directive" (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures intended to ensure a common high level of network and information system security in the Union).

One of the main obligations arising from the NIS2 directive and law is the obligation to provide information and notify incidents. This obligation aims to provide assistance to the entities concerned, to inform the various competent authorities appropriately, to disseminate warning messages about certain threats to other entities and to collaborate at national or European level.

The purpose of this document is to provide general information on the notifications and information requirements under the NIS2 law, which entered into force on 18th October 2024.

Table of contents

A. Mandatory notifications

A.1. WHAT EVENTS MUST BE NOTIFIED BY ENTITIES SUBJECT TO THE NIS2 LAW?

Notification of an event is mandatory when it constitutes a "significant" incident. This involves two elements.

Firstly, it must be **an incident** as defined in art. 8, 5° of the NIS2 law: "an event compromising the availability, authenticity, integrity or confidentiality of data stored, transmitted or being processed, or of services that networks and information systems offer or make accessible".

Secondly, the incident must amount to **a significant incident** as defined in art. 8, 57° of the NIS2 law: "any incident which has a significant impact on the provision of one of the services provided in the sectors or sub-sectors listed in annexes I and II of the NIS2 law and which:

1° has caused or is likely to cause severe operational disruption to any of the services provided in the sectors or sub-sectors listed in annex I and II or financial loss to the entity concerned; or
2° has affected or is likely to affect other natural or legal persons by causing considerable material, physical or moral damage".

A.2. HOW DO YOU DETERMINE WHETHER OR NOT AN INCIDENT IS SIGNIFICANT?

Firstly, the incident (see definition above) must have an impact on the provision of one of the services provided in the sectors or sub-sectors listed in annexes I and II to the law, i.e. it must **affect the networks and information systems that support the provision of one or more of these services** (e.g. electricity distribution).

The mandatory notifications therefore only concern the networks and information systems on which the entity concerned depends to provide the service(s) listed in the annexes of the law. An incident only affecting an isolated information system unrelated to the provision of the aforementioned services therefore does not have to be notified.

Secondly, the impact must be significant, i.e. cause or be likely to cause at least one of these three situations:

- **severe operational disruption to one of the services provided** (in the sectors or sub-sectors listed in annexes I and II to the NIS2 law);
- **financial losses for the entity concerned**;
- **considerable material, physical or moral damage to other natural or legal persons**.

To guide entities in this assessment, the CCB has identified several concrete situations below in which the significant character of an incident should, at the very least, be considered as established by an entity.

However, the situations described are neither exhaustive, nor limited to the various significant incidents that could occur.

1) A suspected malicious event compromising the authenticity, integrity, or confidentiality of data on the entity's networks or information systems, which causes or is likely to cause severe operational disruption

Such an event could occur when (one of these circumstances is sufficient):

- someone has obtained greater access than expected to the networks, systems or information supporting the provision of the entity's service(s);
- a system or network supporting the provision of the entity's service(s) has been or may be configured by a person who should not have the rights to configure the entity's system or network;
- a system or network supporting the provision of the entity's service(s) can no longer be configured by privileged users who should have the rights to configure the system or network;
- configurations or information of the systems supporting the provision of the entity's service(s) have been illegitimately modified, deleted, added, or rendered unreliable;
- a system or network supporting the provision of the entity's service(s) performs tasks it is not supposed to perform or does not perform tasks it is supposed to perform, or does not perform tasks it is supposed to perform related to the access or integrity of the system or network.

For instance, where a cyber threat actor pre-positions itself in a relevant entity’s network and information systems

with a view to causing disruption of services in the future, the incident should be considered to be significant.

2) An event compromising the availability of data on the entity's networks or information systems, which causes or is likely to cause severe operational disruption

Such an event could occur when:

- at least 20% of users do not have access to the service for at least one hour;
- users lose access to the service for at least one hour and the entity cannot determine the number of users affected (in relative or absolute terms);
- the event causes a delay in the delivery of products beyond the contractually guaranteed delivery times.

In case of a planned maintenance shutdown, there is no incident if the impact is limited to what was planned.

The term "user" should be understood to mean the natural and/or legal persons, professional customers and/or end customers who have entered into contract with the entity concerned, giving them access to the relevant service or data, and who have suffered or are likely to suffer the consequences of the incident. To calculate the number of users affected, the number of natural or legal persons, business customers or end customers affected must be taken into account.

The duration of an incident which impacts availability of a service should be measured from the disruption of the proper provision of such service until the time of recovery. Where a relevant entity is unable to determine the moment when the disruption began, the duration of the incident should be measured from the moment the incident was detected, or from the moment when the incident was recorded in network or system logs or other data sources, whichever is earlier.

Limited availability should be considered to occur in particular when a service provided by a relevant entity is considerably slower than average response time, or where not all functionalities of a service are available. Where possible, objective criteria based on the average response times of services provided by the relevant entities should be used to assess delays in response time. A functionality of a service may be, for instance, a chat functionality or an image search functionality.

3) An event causing or likely to cause financial loss to the entity

Such an event could occur when it causes:

- a direct financial loss in excess of €250,000 or 5% of the total annual turnover of the entity concerned during the previous full financial year, whichever is the lower;
- the loss or dissemination of intellectual property in a way likely to jeopardise future revenues or turnover;
- the exfiltration of trade secrets within the meaning of Article 2(1)(1) of Directive (EU) 2016/943 from the entity concerned.

To determine the direct financial losses resulting from an incident, the entities concerned must take into account all the financial losses they have suffered as a result of the incident, such as:

- costs for replacement or relocation of software;
- hardware or infrastructure;
- staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills;
- fees due to non-compliance with contractual obligations;
- costs for redress and compensation to customers, losses due to forgone revenues;
- costs associated with internal and external communication;
- advisory costs, including costs associated with legal counselling;
- forensic services and remediation services;
- other costs associated to the incident.

However, administrative fines, as well as costs that are necessary for the day-to-day operation of the business, should not be considered as financial losses resulting from an incident. These include, but are not limited to:

- costs for general maintenance of infrastructure, equipment, hardware and software;

- keeping skills of staff up to date;
- internal or external costs to enhance the business after the incident, including upgrades;
- improvements and risk assessment initiatives;
- and insurance premiums.

The relevant entities should calculate the amounts of financial losses based on available data and, where the actual amounts of financial losses cannot be determined, the entities should estimate those amounts.

4) An event causing or likely to cause material, physical or moral damage affecting other natural or legal persons

Such an event could occur when it causes:

- partial or total destruction of physical or digital assets;
- damage to physical infrastructure causing a delay in the delivery of products or services beyond the contractually guaranteed delivery times;
- damage such as death, hospitalisation, injury or disability;
- substantial financial consequences.

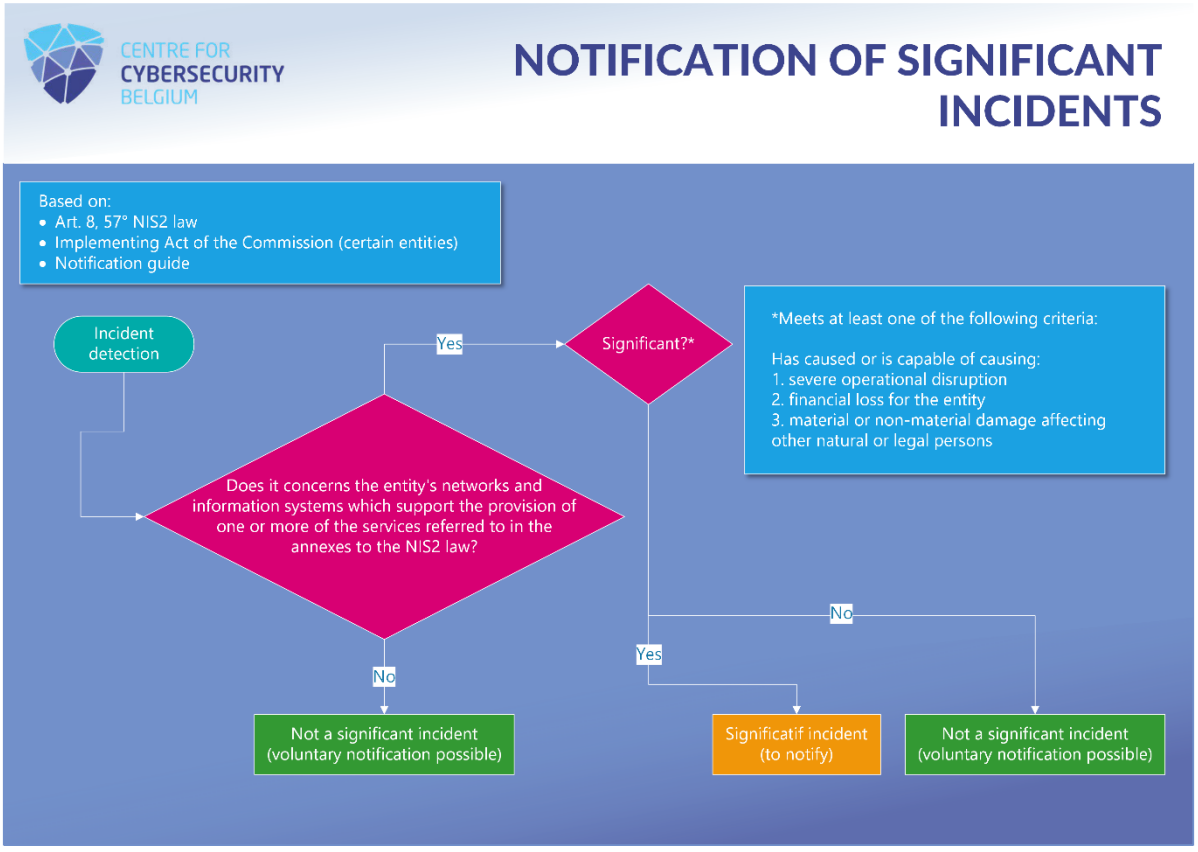
Relevant entities should also be obliged to report incidents that have caused or are capable of causing the death of natural persons or considerable damage to natural persons' health as such incidents are particularly serious cases of causing considerable material or non-material damage. For instance, an incident affecting a relevant entity could cause unavailability of healthcare or emergency services, or the loss of confidentiality or integrity of data with an effect on the health of natural persons.

For the purpose of determining whether an incident has caused or is capable of causing considerable damage to a natural person's health, relevant entities should take into account whether the incident caused or is capable of causing severe injuries and ill-health. For that purpose, the relevant entities should not be required to collect additional information to which they do not have access.

5) A recurring event

Recurring incidents that are linked through the same apparent root cause, which individually do not meet the criteria of a significant incident, should collectively be considered to be a significant incident, provided that they collectively meet the criterion for financial loss, and that they have occurred at least twice within six months.

Such recurring incidents can indicate significant deficiencies and weaknesses in the relevant entity's cybersecurity risk management procedures and their level of cybersecurity maturity. Moreover, such recurring incidents are capable of causing significant financial loss for the relevant entity.



A.3. ARE THERE ANY SPECIAL RULES?

In the implementing act of 17th October 2024[1], the European Commission has specified the criteria for assessing if an incident is considered as "significant" for the following types of entities:

- DNS service providers;
- TLD name registries;
- cloud computing service providers;
- data centre service providers;
- content delivery network providers;
- managed service providers;
- managed security service providers;
- providers of online marketplaces;
- providers of online search engines;
- providers of social networking services platforms;
- trust service providers.

For the entities concerned by the implementing act, these specific rules apply (see annex 3). In the event of contradiction between this guide and the provisions of the implementing act, the latter shall prevail for these entities.

Entities in the banking and financial market infrastructure sectors within the meaning of annex I of the NIS2 Law, which fall within the scope of Regulation (EU) 2022/2554 of 14 December 2022 on the digital operational resilience of the financial sector (DORA), including the activity of central securities depository carried out by the National Bank of Belgium, are not subject to the above-mentioned notification procedures.[2]

In addition, electronic communication operators identified as critical use the escalation matrix established by BIPT and implement the means of redundancy provided for therein. Furthermore, articles 34 and 35 of the NIS2 Law should be interpreted as requiring an early warning notification as soon as possible when the underlying incident

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI_COM:C(2024)7151
[2] Art. 6, § 3 of the NIS2 law.

affects the availability of emergency communications as referred to in article 2, 60° of the law of 13 June 2005 on electronic communications, given the importance of these communications and the impact that the unavailability of these communications may have on the life or physical integrity of persons.

A.4. HOW QUICKLY MUST A SIGNIFICANT INCIDENT BE NOTIFIED?

The notification deadlines are running from the moment the entity becomes aware of such significant incidents. The relevant entity is therefore required to report incidents that, based on its initial assessment, could cause severe operational disruption of the services or financial loss for that entity or affect other natural or legal persons by causing considerable material or non-material damage.

Therefore, when a relevant entity has detected a suspicious event, or after a potential incident has been brought to its attention by a third party, such as an individual, a customer, an entity, an authority, a media organisation, or another source, the relevant entity should assess in a timely manner the suspicious event to determine whether it constitutes an incident and, if so, determine its nature and severity. The relevant entity is therefore to be regarded as having become “aware” of the significant incident when, after such initial assessment, that entity has a reasonable degree of certainty that a significant incident has occurred.

As soon as a NIS2 entity is reasonably aware that it is facing a significant incident, it must notify the national CSIRT (the CCB). There are several stages to this notification[3] :

1) **without undue delay and, in any event, within 24 hours** of becoming aware of the significant incident, the entity submits an early warning;
2) **without undue delay and, in any event, within 72 hours (24 hours for trusted service providers) of becoming aware of the significant incident**, the entity submits an incident notification;
3) at the request of the national CSIRT or, where appropriate, the competent sectoral authority, the entity submits an intermediate report;
4) **no later than one month after the notification of the incident** referred to in point 2, the entity shall submit a final report;
5) should the incident still be ongoing at the time of submission of the final report, the entity concerned submits a progress report and then, within one month of the incident being dealt with, a final report.

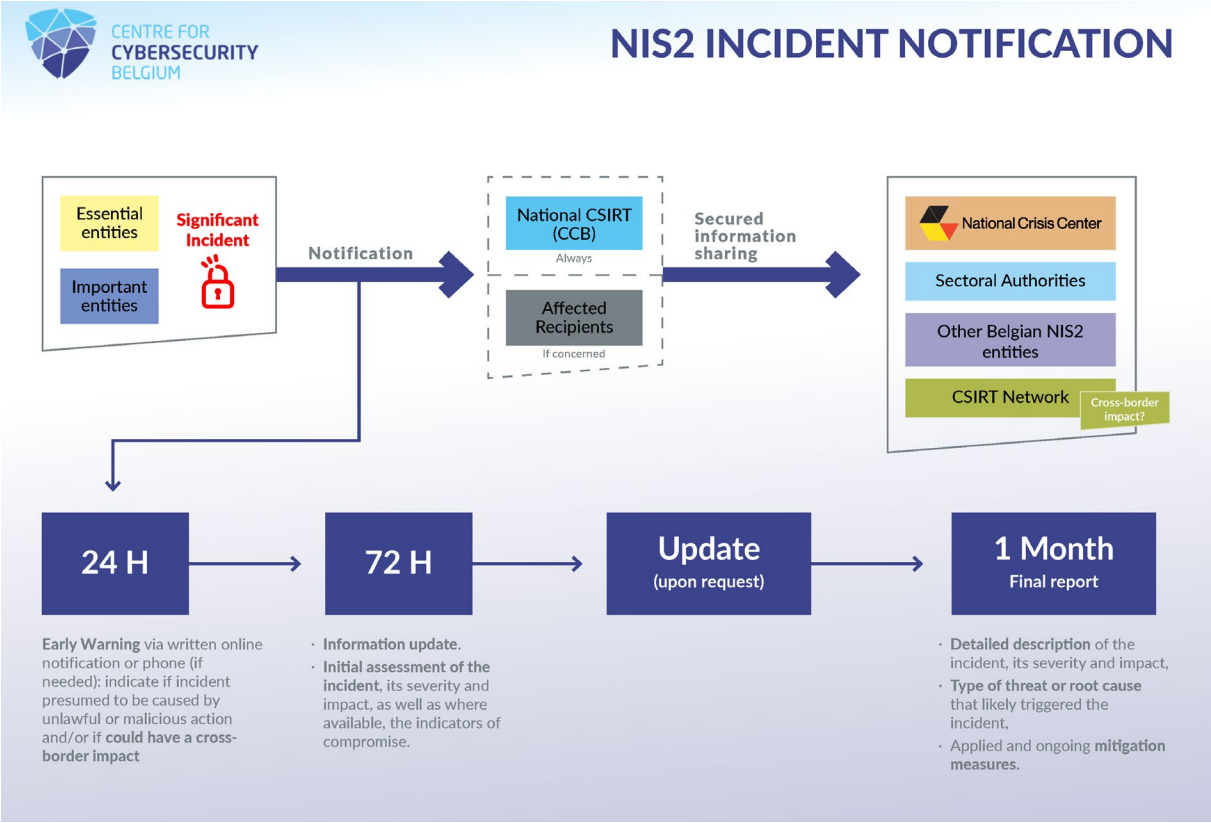
The term "without undue delay" means that the entity in a position to do so must notify the incident as soon as possible, without waiting for the maximum deadlines of 24 hours and 72 hours. Only duly justified special circumstances may lead to waiting until the very end of these deadlines. Compliance with the organisation's internal procedures must not lead to an unreasonable delay in notifying the incident.

Where the significant incident is likely to affect the provision of the services listed in the annexes to the law, the entity must also inform, without undue delay, the recipients of its services (insofar as they are identifiable). This information obligation may be fulfilled by any available means (information on the website, mailing list, message in an application, paper communications, etc).

The NIS2 entity must also communicate, without undue delay, to the recipients of its services potentially affected by a significant cyber-threat (see the definition given below in the voluntary notification section) any measures or corrections that these recipients may apply in response to this threat.

The CCB may share information received by the entity with other authorities to the extent necessary.

[3] Art. 35 of the NIS2 law and the visual below.



A.5. HOW SHOULD THE ENTITY REPORT AN INCIDENT?

For each of the stages mentioned in the previous point, notification is made by the entity concerned using an online form: **https://notif.safeonweb.be** (unless unavailable or technically impossible). The various fields of the online notification form are explained in annex 2 of this guide.

In order to avoid possible obstacles to notification and given the presumed emergency situation in which any entity finds itself, the use of the notification tool does not require prior authentication.

An emergency telephone number **(+32 (0)2 501 05 60)** is also available for NIS2 entities only. The purpose of this channel is to enable entities that so wish to contact the national CSIRT in an emergency should immediate intervention by the national CSIRT be required in the event of an incident. If the form is unavailable or technically impossible to reach for the entity, such an emergency telephone call may be considered equivalent to the notifications referred to in article 35 of the NIS2 law, but the entity may be asked to complete it in writing afterwards for the sake of completeness of information.

A.6. INFORMATION TO BE PROVIDED WHEN A SIGNIFICANT INCIDENT IS REPORTED

The various notification stages involve different types of information to be submitted (see the online form):

- The **early warning** indicates whether it is suspected that the significant incident may have been caused by illicit or malicious acts or whether it may have a cross-border impact (i.e. an impact in another EU country). This early warning includes only the information necessary to bring the incident to the attention of the CSIRT, and enables the entity concerned to request assistance, if necessary.
  Such an alert should not divert the reporting entity's resources from incident management activities that should have the priority.
- The **incident notification** within 72 hours has the purpose to update the information communicated as part of the early warning. It also provides an initial assessment of the incident, including its severity and impact, as well as indicators of compromise (IOCs), where available.
  As with the early warning, incident reporting should not divert the entity's resources from the management of significant incidents.
- The **intermediate report** contains relevant updates on the situation.

- The **final report** should include a detailed description of the incident, including its severity and impact; the type of threat or root cause that is likely to have triggered the incident; the mitigation measures applied and in progress; and where relevant, the cross-border impact of the incident.
- The **progress report** contains as much of the information as possible that should be in the final report and that is in the entity's possession at the time the progress report is submitted.

B. Voluntary notifications

Essential and important entities can report (non-significant) incidents, cyber-threats and near misses.

A cyber-threat means “any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons”.[4]

A near miss means “an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialize”.[5]

Entities that are neither essential nor important can report significant incidents, cyber-threats and near misses.

These voluntary notifications are processed in the same way as mandatory notifications, but mandatory notifications may nevertheless be given priority.

A voluntary notification does not have the direct effect of leading to an inspection of the entity that issued the notification or of imposing additional obligations on it to which it would not have been subject had it not issued the notification.[6]

C. Confidentiality rules applying to information sent via notification

The NIS2 entity and its subcontractors restrict access to information relating to incidents, within the meaning of the NIS2 law, to only those persons who need to know and need to have access to it in order to carry out their functions or duties in relation to this law. This rule also applies to the CCB (as national CSIRT), the National Crisis Centre (NCCN) and any competent sectoral authority.

Notifications are shared immediately by the national CSIRT with any competent sector authorities, and with the NCCN when the notification comes from an essential entity.[7]

Information provided to the CCB, the NCCN and the sectoral authority by a NIS2 entity may be exchanged in an anonymised manner with authorities of other Member States of the European Union and with other Belgian authorities when this exchange is necessary for the application of legal provisions.

However, this transmission of information is limited to what is relevant and proportionate to the purpose of this exchange, in compliance with EU Regulation 2016/679 (GDPR), the confidentiality of the information concerned, security and the commercial interests of the NIS2 entities.

[4] Art. 8, 10° of the NIS2 Law and art. 2, point 8), of Regulation (EU) 2019/881 - "CSA".
[5] Art. 8, 6° of the NIS2 law.
[6] Art. 38, § 2, sub-para. 3 of the NIS2 law - without prejudice to the prevention, detection, investigation and prosecution of criminal offences.
[7] Art. 34 of the NIS2 law.

D. What happens if an incident occurs that also involves personal data?

As is already the case, incident notifications under the NIS2 law do not replace any notifications in the event of a personal data breach, for example to the Data Protection Authority (DPA). Two separate notifications will still be required.

However, the law provides for closer collaboration between the national cybersecurity authority and the data protection authorities. This collaboration could lead to the development of common tools.

The DPA can be notified via their website.[8]

[8] https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles.

Annex 1 - Summary table - significant incident

Type of event	Examples
A **suspected malicious event compromising the authenticity, integrity or confidentiality of data on the entity's networks or information systems, which causes or is likely to cause severe operational disruption.**	• someone has obtained greater access than expected to the networks, systems or information supporting the provision of the entity's service(s); • a system or network supporting the provision of the entity's service(s) has been or may be configured by a person who should not have the rights to configure the entity's system or network; • a system or network supporting the provision of the entity's service(s) can no longer be configured by privileged users who should have the rights to configure the system or network; • configurations or information of the systems supporting the provision of the entity's service(s) have been illegitimately modified, deleted, added, or rendered unreliable; • a system or network supporting the provision of the entity's service(s) performs tasks it is not supposed to perform or does not perform tasks it is supposed to perform related to the access or integrity of the system or network.
An event compromising the availability of data on the entity's networks or information systems, which causes or is likely to cause severe operational disruption.	• at least 20% of users do not have access to the service for at least one hour; • users lose access to the service for at least one hour and the entity cannot determine the number of users affected (in relative or absolute terms); • the event causes a delay in the delivery of products beyond the contractually guaranteed delivery times; • planned maintenance operations should not be taken into account (e.g. planned maintenance shutdowns).
Financial losses for the entity concerned	• a direct financial loss in excess of €250,000 or 5% of the total annual turnover of the entity concerned during the previous full financial year, whichever is the lower; • the loss or dissemination of intellectual property in a way likely to jeopardise future revenues or sales; • the exfiltration of trade secrets within the meaning of Article 2(1)(1) of Directive (EU) 2016/943 from the entity concerned.
Considerable material, physical or moral damage to other natural or legal persons	• partial or total destruction of physical or digital assets; • damage to physical infrastructure causing a delay in the delivery of products beyond the contractually guaranteed delivery times; • damage such as death, hospitalisation, injury or disability; • substantial financial consequences.
Recurring events	• at least twice within a six-month period; • related to the same apparent root cause; • meet collectively the criteria of financial loss (to the entity or to third parties) or unavailability.

Annex 2 - Explanation of the notification form

The various fields in the notification form are described below. The left-hand column contains the technical title of the field (in square brackets) and the title visible to users (in bold). The right-hand column contains the field description. The fields are divided into sections, each with its own technical title (in square brackets and capitalised).

[ENTITY NOTIFYING THE INCIDENT]	
[Field Name: Submitter] **Concerning...**	This field allows you to indicate whether you are a NIS2 entity (mandatory field).
[SPECIFIC CHARACTERISTICS NIS]	
[Field Name: NIS_Type] **How is the organisation defined under the NIS2 law?**	This field allows you to indicate whether you are an important or essential entity within the meaning of the NIS2 law (mandatory field).
[Field Name: Sector] **In which main sector(s) does your organisation operate?**	This field allows you to indicate the sector(s) in which you are active. It is possible to tick more than one box (mandatory field).
[Field Name: NIS_Notification] **What type of NIS2 incident notification are you submitting?**	This field allows you to indicate the stage of the notification process you are at. As a reminder, the stages are described in point A. "How quickly must a significant incident be notified?" (mandatory field).
[INCIDENT DETAILS]	
[Field Name: Tracking_Reference] **Tracking Reference**	This field allows you to indicate a tracking reference if you have already received one from the CCB (optional field).
[Field Name: Malicious_Intent] **Do you believe this incident is the result of malicious intent?**	This field allows you to indicate whether you think the incident was malicious. If you do not know or are not convinced, please tick "Uncertain" (mandatory field).
[Field Name: Incident_Type] I**ncident type**	This field allows you to choose from a list of incident types the one or ones that correspond to the incident you wish to notify. It is possible to tick several boxes (mandatory field).
[Field Name: Incident_Date] **When did the incident take place?**	This field allows you to enter the date in Month/Day/Year format. If you are unsure, the following field (I.) can be used to provide any information you have about when the incident took place (optional field).

[Field Name: Incident_Description] **Describe the incident (initial cause, impact to organization, virus/malware name, data and systems affected, actions taken, operating systems/software involved, etc.)**	This field allows you to provide the information in your possession relating to the incident, including indicators of compromise. To find out which information should be given priority, please refer to point A. "Information to be provided when a significant incident is reported", which describes the information to be provided for each stage of notification. Please note that the form includes specific fields for the causes, consequences and severeness of the incident. You have a maximum of 500 characters (mandatory field).
[Field Name: Assessment_Severity] **Please provide an assessment of the severity of the incident**	This field allows you to describe the severeness of the incident. In the context of early warning, such an assessment may be very brief and/or partial. As part of the notification within 72 hours of the incident, you must provide an initial assessment of the severeness of the incident. As part of the final report, this assessment must be detailed. You have a maximum of 500 characters (mandatory field).
[Field Name: Assessment_Consequence] **What are the consequences of the incident?**	This field allows you to describe the impact of the incident. In the context of early warning, such an assessment may be very brief and/or partial. As part of the notification within 72 hours of the incident, you must provide an initial assessment of the impact of the incident. As part of the final report, this assessment must be detailed. Please note that the form includes specific fields on the potential cross-border impact of the incident. You have a maximum of 500 characters (mandatory field).
[Field Name: Threat_Type_Root_Cause] **What caused the incident?**	This field allows you to indicate whether the cause of the incident is known and, if so, to provide information about it. Please note that at the final report stage, you must indicate the type of threat or root cause that probably triggered the incident. You have a maximum of 500 characters (mandatory field).
[Field Name: Cross_Border_Impact] **Do you believe this incident might lead to cross-border issues?**	This field allows you to indicate whether you think the incident has a cross-border impact. If you do not know or are not sure, tick "Uncertain". Please note that at the final report stage, you must indicate, if applicable, the cross-border impact of the incident (mandatory field).
[Field Name: Cross_Border_Impact_Description] **Provide details of the cross-border issues this incident might provoke**	This field allows you to provide details of the cross-border impact of the incident. Please note that this field only appears if you have ticked "Yes" in the previous field (M.) (optional field).
[Field Name: Police_Involved] **Have you reported the incident to the police? (If you have been the victim of a successful cyber-attack, we advise you to report it to the police)**	This field allows you to indicate whether you have already reported the incident to the police. It is advisable to do so if the incident is malicious or intentional (optional field).

[Field Name: Help_Needed] **Do you need support, analysis or advice from the CCB?**	This field allows you, where appropriate, to expressly request support from the CCB by ticking the yes box. This support consists of operational guidance or advice on the implementation of possible mitigation measures, or even additional technical support (mandatory field).
[Field Name: Help_Type_Needed] **Specify as precisely as possible the support you need from the CCB:**	This field allows you to describe the type of support you would require in the management of the incident giving rise to the notification. This support consists of operational guidance or advice on the implementation of possible mitigation measures, or even additional technical support. Maximum 500 characters (mandatory field).
[Field Name: Actions_Taken] **What actions did you take?**	This field allows you to describe the measures taken to mitigate and/or remedy the incident. Please note that this field is optional, but as part of the final report, you must describe the mitigation measures applied and in progress. You have 500 characters (optional field).
[Field Name: Resolved] **Is the incident now resolved?**	This field allows you to indicate whether the incident has been resolved at the time of notification (mandatory field).
[FURTHER INFORMATION]	
[Field Name: Incident_Detection_Date] **When was the incident detected?**	This field allows you to indicate when the incident has been detected (mandatory field).
[Field Name: Incident_Detection_Description] **How was the incident detected?**	This field allows you to indicate how you managed to discover the incident (mandatory field).
[Field Name: Incident_Detection_Timeline] **Provide a detailed timeline with all actions taken.**	This field allows you to indicate when you took which actions (mandatory field).
[Field Name: Incident_Detection_Communication] **Which communication occurred in response to the incident? With whom, time of communication, brief content, mode (oral/mail/written) or reference.**	This field allows you to indicate who you informed about what, when, with sufficient details to be able to trace back all necessary communications about the incident (mandatory field).
[Field Name: Incident_Detection_Preventive_Measures] **What preventive measures were in place at the time of the incident? (This refers to measures which already existed but did not help)**	This field allows you to indicate what cybersecurity measures which were already in place when the incident happened, and which were insufficient to counter it (mandatory field).
[Field Name: Incident_Detection_Corrective_Measures] **What**	This field allows you to indicate what cybersecurity measures you took after noticing the incident, to stop it

corrective measures were taken as a result of the incident? (This refers to measures taken immediately to stop the incident)	(mandatory field).
[Field Name: Incident_Detection_Lessons_Learned] **What lessons were learned from the incident?**	This field allows you to indicate the things you have learned after the incident has passed (mandatory field).
[Field Name: Incident_Detection_New_Measures] **What new (adapted) preventive measures were implemented after the incident?**	This field allows you to indicate what new preventive measures you have implemented after the incident, and what measures you have adapted to counter a new incident (mandatory field).
[Field Name: MFA_Applied] **Was MFA applied to your impacted environment when the incident occurred?**	This field allows you to specify whether Multi-Factor Authentication (MFA) was applied before the incident took place (mandatory field).
[ENTITY CONTACT DETAILS]	
[Field Name: Anonymous]	This field is not visible and indicates whether the notification is made anonymously.
[Field Name: Contact_Person] **Point of contact**	This field allows you to enter the name of the contact person for incident management purposes (optional field).
[Field Name: Organization] **Organisation name**	This field allows you to indicate the name of the organisation on whose behalf the notification is being made (mandatory field).
[Field Name: Email] **Email**	This field allows you to enter the email address that can be used by the CCB to contact the organisation that is the victim of the incident (mandatory field).
[Field Name: Telephone] **Telephone**	This field allows you to indicate the telephone number that can be used by the CCB to contact the organisation that is the victim of the incident (mandatory field).
[Field Name: Location] **Where did the incident take place?**	This field allows you to indicate where the incident took place (optional field).

Annex 3 - Summary of the rules of the Commission Implementing Regulation of 17 October 2024 (2024/2690) on the notification of significant incidents

An entity subject to the Commission Implementing Regulation of 17 October 2024 must consider an incident as "significant" when either one of the circumstances common to all entities or one of the specific circumstances mentioned below occurs.	
Circumstances common to all entities subject to the Implementing Regulation (art. 3) Scheduled interruptions of service and planned consequences of scheduled maintenance operations carried out by or on behalf of the relevant entities shall not be considered to be significant incidents.	
Financial losses for the entity concerned	(a) the incident has caused or is capable of causing direct financial loss for the relevant entity that exceeds EUR 500 000 or 5 % of the relevant entity's total annual turnover in the preceding financial year, whichever is lower; (b) the incident has caused or is capable of causing the exfiltration of trade secrets as set out in Article 2, point (1), of Directive (EU) 2016/943 of the relevant entity.
Considerable material, physical or moral damage to other natural or legal **persons**	c) the incident has caused or is capable of causing the death of a natural person; d) the incident has caused or is capable of causing considerable damage to a natural person's health.
A suspected malicious event compromising the authenticity, integrity or confidentiality of data on the entity's networks or information systems, which causes or is likely to cause serious operational disruption	(e) a successful, suspectedly malicious and unauthorised access to network and information systems occurred, which is capable of causing severe operational disruption.
Recurring event (art. 4)	(f) Incidents that individually are not considered a significant incident within the meaning of Article 3, shall be considered collectively as one significant incident where they meet all of the following criteria: - they have occurred at least twice in six months; - they have the same apparent root cause; - they collectively meet the criteria set out in Article 3(1)(a). [The incident has caused or is capable of causing direct financial loss for the relevant entity that exceeds EUR 500 000 or 5 % of the relevant entity's total annual turnover in the preceding financial year, whichever is lower].

Specific circumstances by type of entity (art. 5 to 14)

When calculating the number of users impacted by an incident for the purpose of Articles 7 and 9 to 14, the relevant entities shall consider all of the following:

(a) the number of customers that have a contract with the relevant entity which grants them access to the relevant entity's network and information systems or services offered by, or accessible via, those network and information systems;

(b) the number of natural and legal persons associated with business customers that use the entities' network and information systems or services offered by, or accessible via, those network and information systems.

DNS service providers (art. 5)

(a) a recursive or authoritative domain name resolution service is completely unavailable for more than 30 minutes;
(b) for a period of more than one hour, the average response time of a recursive or authoritative domain name resolution service to DNS requests is more than 10 seconds;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the authoritative domain name resolution service is compromised, except in cases where the data of fewer than 1 000 domain names managed by the DNS service provider, amounting to no more than 1 % of the domain names managed by the DNS service provider, are not correct because of misconfiguration.

TLD name registries (Art. 6)

(a) an authoritative domain name resolution service is completely unavailable;
(b) for a period of more than one hour, the average response time of an authoritative domain name resolution service to DNS requests is more than 10 seconds;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the technical operation of the TLD is compromised.

Cloud computing service providers (art. 7)

(a) a cloud computing service provided is completely unavailable for more than 30 minutes;
(b) the availability of a provider's cloud computing service is limited for more than 5% of the users of that service in the Union, or for more than 1 million users of that service in the Union, whichever is the smaller, for more than one hour;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a cloud computing service is compromised as a result of a suspectedly malicious action;
(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a cloud computing service is compromised with an impact on more than 5 % of that cloud computing service's users in the Union, or on more than 1 million of that cloud computing service's users in the Union, whichever number is smaller.

Data centre service providers (art. 8)

(a) a data centre service of a data centre operated by the provider is completely unavailable;
(b) the availability of a data centre service of a data centre operated by the provider is limited for a duration of more than one hour;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a data centre service is compromised as a result of a suspectedly malicious action;
(d) physical access to a data centre operated by the provider is compromised.

Content delivery network providers (art. 9)

(a) a content delivery network is completely unavailable for more than 30 minutes;
(b) the availability of a content delivery network is limited for more than 5 % of the content delivery network's users in the Union, or for more than 1 million of the content delivery network's users in the Union, whichever number is smaller, for a duration of more than one hour;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a content delivery network is compromised as a result of a suspectedly malicious action;
(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a content delivery network is compromised with an impact on more than 5 % of that content delivery network's users in the Union, or on more than 1 million of that content delivery network's users in the Union, whichever number is smaller.

Managed service providers and managed security service providers (art. 10)

(a) a managed service or managed security service is completely unavailable for more than 30 minutes;
(b) the availability of a managed service or managed security service is limited for more than 5 % of the service's users in the Union, or for more than 1 million of the service's users in the Union, whichever number is smaller, for a duration of more than one hour;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a managed service or managed security service is compromised as a result of a suspectedly malicious action;
(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a managed service or a managed security service, is compromised with an impact on more than 5 % of that managed service's or that managed security service's users in the Union, or on more than 1 million of the service users in the Union, whichever number is smaller.

Providers of online marketplaces (art. 11)

(a) an online marketplace is completely unavailable for more than 5 % of an online marketplace's users in the Union, or for more than 1 million of an online marketplace's users in the Union, whichever number is smaller;
(b) more than 5 % of an online marketplace's users in the Union, or more than 1 million of an online marketplace's users in the Union, whichever number is smaller, are impacted by limited availability of that online marketplace;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online marketplace is compromised as a result of a suspectedly malicious action;
(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online marketplace is compromised with an impact on more than 5 % of that online marketplace's users in the Union, or on more than 1 million of that online marketplace's users in the Union, whichever number is smaller.

Providers of online search engines (art. 12)

(a) an online search engine is completely unavailable for more than 5 % of that online search engine's users in the Union, or for more than 1 million of that online search engine's users in the Union, whichever number is smaller;
(b) more than 5 % of an online search engine's users in the Union, or more than 1 million of an online search engine's users in the Union, whichever number is smaller, are impacted by limited availability of that online search engine;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online search engine is compromised as a result of a suspectedly malicious action;
(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online search engine is compromised with an impact on more than 5 % of that online search engine's users in the Union, or on more than 1 million of that online search engine's users in the Union, whichever number is smaller.

Providers of social network service platforms (art. 13)

(a) a social networking service platform is completely unavailable for more than 5 % of that social networking service platform's users in the Union, or for more than 1 million of that social networking service platform's users in the Union, whichever number is smaller;
(b) more than 5 % of a social networking service platform's users in the Union, or more than 1 million of a social networking service platform's users in the Union, whichever number is smaller, are impacted by limited availability of that social networking service platform;
(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a social networking service platform is compromised as a result of a suspectedly malicious action;
(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a social networking service platform is compromised with an impact on more than 5 % of that social networking service platform's users in the Union, or on more than 1 million of that social networking service platform's users in the Union, whichever number is smaller.

Trust service providers (art. 14)

(a) a trust service is completely unavailable for more than 20 minutes;
(b) a trust service is unavailable to users, or relying parties, for more than one hour calculated on a calendar week basis;
(c) more than 1 % of the users or relying parties in the Union, or more than 200 000 users or relying parties in the Union, whichever number is smaller, are impacted by limited availability of a trust service;
(d) physical access to an area where network and information systems are located and to which access is restricted to trusted personnel of the trust service provider, or the protection of such physical access, is compromised;
(e) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a trust service is compromised with an impact on more than 0,1 % of users or relying parties, or more than 100 of users or relying parties, whichever number is smaller, of the trust service in the Union.

NIS2 NOTIFICATION GUIDE

Responsible editor:
Centre for Cybersecurity Belgium
M. De Bruycker, Director General
Rue de la loi, 18
1000 Brussels

Legal deposit:
D/2024/14828/013