



Incident notification form for digital service providers

As referenced in Section 13, subsection 1b of the Security of Network and Information Systems Act (Wbni).

Please complete this form as fully as possible. Incidents must be reported immediately upon discovery. Please send your completed form securely to [wbni@agentschaptelecom.nl](mailto:wbnl@agentschaptelecom.nl).

o. The following fields must be completed for new notifications

o.1 General notification information

Must be completed for new notifications.

Incident notification date and time	
New/follow-up notification	<input type="checkbox"/> New notification <input type="checkbox"/> Supplement/amendment to existing notification <input type="checkbox"/> Incident closure notification
Incident status	<input type="checkbox"/> Incident ongoing <input type="checkbox"/> Incident closed <input type="checkbox"/> Withdrawn

o.2 Reporting party information

Must be completed for new notifications.

Digital service provider	Company name	
	Company address	
	Chamber of Commerce (KvK) number	
	Type	<input type="checkbox"/> Online marketplace <input type="checkbox"/> Online search engine <input type="checkbox"/> Cloud computing service
Reporting official	Name	
	Position	
	Email address	
	Telephone number	
	Availability	



Contact official Complete this field if the contact official is not the same as the reporting official.	Name	
	Position	
	Email address	
	Telephone number	

0.3 Incident information

Must be completed for new notifications to satisfy the statutory notification obligation.

Incident discovery date and time	
Incident description	
Significant impact	

1. The following fields may be completed later

1.1 Description of the incident from an ICT perspective

These fields may be completed after the initial notification.

Impact category More than one answer may be given.	<input type="checkbox"/> Availability <input type="checkbox"/> Integrity <input type="checkbox"/> Confidentiality <input type="checkbox"/> Authenticity		
Affected essential service components in your organisation More than one answer may be given.	<input type="checkbox"/> Online marketplace <input type="checkbox"/> Software <input type="checkbox"/> Hardware <input type="checkbox"/> System <input type="checkbox"/> Data <input type="checkbox"/> Persons	<input type="checkbox"/> Online search engine <input type="checkbox"/> Software <input type="checkbox"/> Hardware <input type="checkbox"/> System <input type="checkbox"/> Data <input type="checkbox"/> Persons	<input type="checkbox"/> Cloud computing service <input type="checkbox"/> Software <input type="checkbox"/> Hardware <input type="checkbox"/> System <input type="checkbox"/> Data <input type="checkbox"/> Persons
What caused the incident More than one answer may be given.	System outage <input type="checkbox"/> Software errors and bugs <input type="checkbox"/> Hardware failure and bugs <input type="checkbox"/> Procedural errors <input type="checkbox"/> Other	Human factor <input type="checkbox"/> Deliberate misuse or mismanagement <input type="checkbox"/> Non-deliberate misuse or mismanagement	Third party <input type="checkbox"/> Supplier <input type="checkbox"/> Subcontractor



	Natural disasters <input type="checkbox"/> Storm <input type="checkbox"/> Earthquake <input type="checkbox"/> Other	Malicious action <input type="checkbox"/> Cyberattack <input type="checkbox"/> Vandalism <input type="checkbox"/> Theft <input type="checkbox"/> Other	
	Explanatory notes		
Start date and time of the incident			
How was the incident discovered?			
Suspected method of attack Complete this field if you ticked one of the "malicious action" boxes above. More than one answer may be given.	<input type="checkbox"/> Exploitation of vulnerabilities	<input type="checkbox"/> Malware	<input type="checkbox"/> Targeted attack
	Explanatory notes	Explanatory notes (e.g. IoCs)	Explanatory notes (e.g. IoCs)
	<input type="checkbox"/> Denial of service	<input type="checkbox"/> Unauthorised access	<input type="checkbox"/> Other
	Explanatory notes (e.g. IoCs)	Explanatory notes	Explanatory notes

1.2 Incident impact

These fields may be completed after the initial notification.

Incident impact in EU Member States More than one answer may be given.	Number of users affected <input type="checkbox"/> The incident has negatively affected more than 100.000 users in the EU. Please provide more information.	
	Explanatory notes	



	Incident duration <input type="checkbox"/> The incident has cost more than 5.000.000 user hours throughout the EU. Please provide more information.	
	Explanatory notes	
	Geographical area <input type="checkbox"/> One or more users in the EU have suffered more than €1.000.000 worth of damage. Please provide more information.	
	Explanatory notes	
	Threat to public safety or public security <input type="checkbox"/> There is a threat to public safety or security. Please provide more information.	
	Explanatory notes	
	Deaths <input type="checkbox"/> The incident has caused at least one death. Please provide more information.	
	Explanatory notes	

1.3 Affected data

These fields may be completed after the initial notification.

Affected data More than one answer may be given.	Personal data <input type="checkbox"/> Yes. Please indicate below which personal data have been affected, specifying any special categories of personal data affected.	
	Explanatory notes	
	Other data s <input type="checkbox"/> Yes. Please indicate below which data have been affected. <input type="checkbox"/> N/A	
	Explanatory notes	



1.4 Notification to other bodies including CSIRT for essential services

These fields may be completed after the initial notification.

Which other bodies did you notify about the incident?	
May Radiocommunications Agency Netherlands share details of your notification with the Cyber Security Incident Response Team for Digital Service Providers (CSIRT DSP)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
May Radiocommunications Agency Netherlands share details of your notification with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens)? <small>Only if personal data have been affected</small>	<input type="checkbox"/> Yes <input type="checkbox"/> No
May Radiocommunications Agency Netherlands share details of your notification with other regulators?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Have you reported the incident to the police? <small>Complete this field if you ticked one of the "Malicious action" boxes above.</small>	<input type="checkbox"/> Yes <input type="checkbox"/> No

1.5 Investigation, measures and residual risk

These fields may be completed after the initial notification.

Incident investigation	Estimated investigation duration	
	Estimated recovery time needed	
	Support from third parties	
Measures	Description of temporary measures	
	Description of structural measures	
Accepted residual risk		



1.6 Other

These fields may be completed after the initial notification.

Estimated impact on affected subsectors <small>More than one answer may be given.</small>	Other digital services <input type="checkbox"/> Online marketplace <input type="checkbox"/> Online search engine <input type="checkbox"/> Cloud computing service Which service has been affected?	Transport <input type="checkbox"/> Air transport <input type="checkbox"/> Rail transport <input type="checkbox"/> Water transport <input type="checkbox"/> Road transport Which essential service has been affected?	Health care <input type="checkbox"/> Health care institutions (including hospitals and private clinics) Which (essential) service has been affected?
	Energy <input type="checkbox"/> Electricity <input type="checkbox"/> Petroleum/Oil <input type="checkbox"/> Gas Which essential service has been affected?	Banking sector <input type="checkbox"/> Banks Which essential service has been affected?	Drinking water suppliers and distributors <input type="checkbox"/> Supplier <input type="checkbox"/> Distributor Which essential service has been affected?
	Vital/non-essential <input type="checkbox"/> Nuclear <input type="checkbox"/> Telecom <input type="checkbox"/> Trust service <input type="checkbox"/> National government <input type="checkbox"/> Water-control structure/management Which service has been affected?	Financial market infrastructure <input type="checkbox"/> Trading platform operator <input type="checkbox"/> Central counterparty Which essential service has been affected?	Digital infrastructure <input type="checkbox"/> Internet hubs <input type="checkbox"/> DNS suppliers <input type="checkbox"/> Register for top-level domain names Which essential service has been affected? As yet unknown <input type="checkbox"/> As yet unknown
Incident closure	Date and time		



	Reason	

Sending this notification form

Please complete this form as fully as possible. Incidents must be reported immediately upon discovery. Please send your completed form securely to wbnl@agentschaptelecom.nl.



Incident notification form for digital service providers – explanatory notes

Pursuant to the Wbni, any cyber security incident with significant impact for your digital service provision must be reported to Radiocommunications Agency Netherlands immediately.

In addition to the required fields, you are requested to complete this form as fully as possible. By completing the required fields (block 0), you satisfy the statutory notification obligation. The information in the other fields (block 1) will help Radiocommunications Agency Netherlands carry out its investigation. It is possible to provide additional information after the initial notification of the incident, after more information has become available. If the information is sensitive, you must send the notification securely.

A cyber security incident is defined as any event having an actual adverse effect on the security of network and information systems. The security of network and information systems is defined as the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality. More specifically, this refers to the availability, integrity, confidentiality and authenticity of stored, transmitted or processed data or the related services offered by or accessible via those network and information systems.

A digital service provider is defined as a legal entity that offers one or more digital services. Such digital services may be online marketplaces, online search engines or cloud computing services. Use the flow chart below to determine whether an organisation is a digital service provider bound by the stipulations of the Security of Network and Information Systems Act (Wbni):



Use the following flow chart to determine whether an incident will have significant impact for your service provision in the European Union.

An incident has occurred



o.1 General notification information

Must be completed for new notifications.

Incident notification date and time	Enter the date and time of this notification. Use the following format when filling in this field dd / mm / yyyy hh: mm (d = day, m = month, y = year, h = hour, m = minute).
New/follow-up notification	Indicate whether this is a new, follow-up or closure notification. An initial notification is for an incident that you have not yet reported to Radiocommunications Agency Netherlands. A follow-up notification is made to provide additional information regarding a previously reported incident.
Incident status	Indicate whether the cause has already been determined and whether the incident is still under investigation. You can also use this field to withdraw an incident notification.

o.2 Reporting party information

Must be completed for new notifications.

Digital service provider	Details of the digital service provider.
Reporting official	Details of the official who reports the incident.
Contact official	Details of the contact official. This may be a different official from the one reporting the incident.



0.3 Incident information

Must be completed for new notifications.

Incident discovery date and time	Indicate the incident discovery date and time as accurately as possible. Use the following format when filling in this field dd / mm / yyyy hh: mm (d = day, m = month, y = year, h = hour, m = minute).
Incident description	Describe the incident. Provide answers to such questions as: which service has been affected and in what way, at which layer of the organisation did the incident take place, how did you establish that an incident had taken place.
Significant impact	Indicate how this incident will affect society.

1.1 Description of the incident from an ICT perspective

These fields may be completed later in a follow-up notification.

Impact category	<p>A security incident may affect one or more of the following factors:</p> <ul style="list-style-type: none"> – availability: the extent to which the service or the information contained therein is active or available when required; – integrity: the extent to which the service or the information contained therein has been amended without authorisation (either by accident or by design); – confidentiality: the guarantee that the service or the information contained therein is only accessible to a certain defined group of authorised users; – authenticity: the extent to which parties can demonstrate that they are involved in a transaction. <p>More than one answer may be given.</p>
Affected essential service components in your organisation	Indicate which part of your service has been affected by the incident. Also, indicate which of the service's ICT components have been affected, if you can. It is possible that multiple ICT components of the same service have been affected.
What caused the incident?	<p>Indicate what caused the incident, if known. More than one answer may be given.</p> <p>Explain your choice(s).</p>
Incident start date and time	Indicate the incident start date and time as accurately as possible. Use the following format when filling in this field dd / mm / yyyy hh: mm (d = day, m = month, y = year, h = hour, m = minute).
How was the incident discovered?	Describe briefly how the incident was discovered, e.g. as a result of a system outage, during system maintenance, during system monitoring, when evaluating log files or auditing results, etc. Use free text to fill in this field.
Suspected method of attack	<p>Indicate how the attack that caused the incident took place. More than one answer may be given. Provide an explanation if you can. Also, indicate in the explanatory notes whether you discovered any indicators of compromise (IoCs). IoCs are indicators that a system or process has been compromised, e.g. hashed values, protocols, IP ports, etc. You do not have to provide the exact IoC(s).</p> <p>Complete this field if you ticked one of the "Malicious action" boxes above, i.e. if the incident was caused by an attack. More than one answer may be given.</p>

1.2 Incident impact

These fields may be completed later in a follow-up notification.

Incident impact in EU Member States	It is important that you indicate the impact of the incident here. Use the flow chart to determine whether an incident will have considerable consequences in EU Member States. More than one answer may be given. Provide an explanation.
--	--



1.3 Affected data

These fields may be completed later in a follow-up notification.

Affected data	Provide an estimation of which data have been affected by the incident. Make specific mention of personal and special personal data.
----------------------	--

1.4 Notification to other bodies including CSIRT for essential services

These fields may be completed later in a follow-up notification.

Which other bodies did you notify about the incident?	Indicate which other bodies you notified about the incident. Also, indicate how and when you did this. Examples of such bodies are CSIRT DSP and the Dutch Data Protection Agency.
May Radiocommunications Agency Netherlands share details of your notification with the Cyber Security Incident Response Team for Digital Service Providers (CSIRT DSP)?	Use this field to give Radiocommunications Agency Netherlands permission to share details of your notification with CSIRT DSP.
May Radiocommunications Agency Netherlands share details of your notification with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens)?	Use this field to give Radiocommunications Agency Netherlands permission to share details of your notification with the Dutch Data Protection Authority. Naturally, you only need to do this if personal data have been affected.
May Radiocommunications Agency Netherlands share details of your notification with other regulators?	Use this field to give Radiocommunications Agency Netherlands permission to share details of your notification with other regulators.
Have you reported the incident to the police?	Indicate whether you reported malicious action/an attack to the police.

1.5 Investigation, measures and residual risk

These fields may be completed later in a follow-up notification.

Incident investigation	Estimated investigation duration	Estimate how much time you will need to investigate the incident (after notification). Use free text to fill in this field.
	Estimated recovery time needed	Estimate how much time you will need to close the incident (after notification).
	Support from third parties	Indicate which third parties and third-party services, if any, you used to resolve the incident and how you used them. Use free text to fill in this field.
Measures	Description of temporary measures	Indicate which measures you have taken to minimise the consequences of the incident. These measures may be temporary.
	Description of structural measures	Proposed measures are defined as the measures you have taken or planned to protect against the incident and its consequences permanently and to prevent a repeat of the incident.
Accepted residual risk	Indicate which risks are not covered by the measures you have taken and how you	



intend to deal with these risks. Use free text to fill in this field.

1.6 Other

These fields may be completed later in a follow-up notification.

Estimated impact on affected subsectors	<p>Estimate the impact of the reported incident on other subsectors mentioned in the Security of Network and Information Systems Act (Wbni). It is vital that the impact of the incident remain limited. If an incident has spread beyond a single environment or service, you must report this here.</p> <p>Under "Which (essential) service has been affected?", indicate which (essential) service in the other subsector has been affected.</p>
Incident closure	<p>When closing or withdrawing the incident, indicate the date, time and reason for doing so.</p>

Sending this notification form

Please complete this form as fully as possible. Incidents must be reported immediately upon discovery. Please send your completed form securely to wbn@agentschaptelecom.nl.