Incident notification form for operators of essential services

As referenced in Section 10, subsections 2 and 3 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.**

0. The following fields must be completed for new notifications

0.1 General notification information

Must be completed for new notifications.

Incident notification date and time	
New/follow-up notification	○ New notification ○ Supplement/amendment to existing notification ○ Incident closure notification
Incident status	○ Incident ongoing ○ Incident closed ○ Withdrawn
How high do you estimate the risk of significant impact? Complete this field if the incident has not yet had significant impact.	○ High ○ Medium ○ Low
What do you estimate the impact of the damage to be when the significant impact come to pass? Complete this field if the incident has not yet had significant impact.	○ High ○ Medium ○ Low

0.2 Reporting party information

Must be completed for new notifications.

Company name		
What type of essential service do you provide?	☐ Electricity ☐ Gas ☐ Petroleum/Oil ☐ TLD (Top Level Domain) ☐ DNS (Domain Name Service) ☐ IX (Internet eXchange)	
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.

Digital service provider incident with significant impact on the continuity of your essential service	○ Yes (state the name of the digital service provide). ○ No
Nature and scope of the incident	
Suspected date and time the incident began	
Potential impact of the incident in The Netherlands and abroad	
Estimated recovery time needed	
Description of measures that have been taken to minimise the impact, if any	
Description of measures that have been taken to prevent the incident recurring, if any	

1. The following fields may be completed later, after the initial notification

1.1 Description of the incident from an ICT perspective

These fields may be completed after the initial notification.

<table>
<tr><td>Incident category
More than one answer may be given.</td><td colspan="3">☐ Availability
☐ Integrity
☐ Confidentiality
☐ Authenticity</td></tr>
<tr><td rowspan="2">Affected essential service components in your organisation
More than one answer may be given.</td><td colspan="3">☐ Software
☐ Hardware
☐ System
☐ Data
☐ Persons</td></tr>
<tr><td>Explanatory notes</td><td colspan="2"></td></tr>
<tr><td rowspan="2">What caused the incident?
More than one answer may be given</td><td>System outage
☐ Software errors and bugs
☐ Hardware failure and bugs
☐ Procedural errors
☐ Other
Natural disasters
☐ Storm
☐ Earthquake
☐ Other</td><td>Human factor
☐ Deliberate misuse or mismanagement
☐ Non-deliberate misuse or mismanagement
Malicious action
☐ Cyberattack
☐ Vandalism
☐ Theft
☐ Other</td><td>Third party
☐ Supplier
☐ Subcontractor</td></tr>
<tr><td>Explanatory notes</td><td colspan="2"></td></tr>
<tr><td>How was the incident discovered?</td><td colspan="3"></td></tr>
<tr><td>Incident discovery date and time</td><td colspan="3"></td></tr>
<tr><td rowspan="3">Suspected method of attack
Complete this field if you ticked one of the "Malicious action" boxes above. More than one answer may be given.</td><td>☐ Exploitation of vulnerabilities</td><td>☐ Malware</td><td>☐ Targeted attack</td></tr>
<tr><td>Explanatory notes</td><td>Explanatory notes (e.g. IoCs)</td><td>Explanatory notes (e.g. IoCs)</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

	☐ **Denial of service**	☐ **Unauthorised access**	☐ **Other**
	Explanatory notes (e.g. IoCs)	Explanatory notes	Explanatory notes

1.2 Affected data

These fields may be completed after the initial notification.

Affected data More than one answer may be given.	**Personal data** ☐ Yes. Please indicate below which personal data have been affected, specifying any special categories of personal data affected.	
	Explanatory notes	
	Other data ◯ Yes. Please indicate below which data have been affected. ◯ N/A	
	Explanatory notes	

1.3 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 operators of essential services, the National Cyber Security Centre (NCSC)?	◯ Yes ◯ No
May Radiocommunications Agency Netherlands share details of your notification with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens)? Only if personal data have been affected.	◯ Yes ◯ No

May Radiocommunications Agency Netherlands share details of your notification with other regulators?	☐ Yes ☐ No
Have you reported the incident to the police? Complete this field if you ticked one of the "Malicious action" boxes above.	☐ Yes ☐ No

1.4 Investigation and residual risk

These fields may be completed after the initial notification.

Incident investigation	Estimated investigation duration	
	Support from third parties	
Accepted residual risk		

1.5 Other

These fields may be completed after the initial notification.

Estimated impact on affected subsectors More than one answer may be given.	**Digital service provider** ☐ Online marketplace ☐ Online search engine ☐ Cloud computing service **Which service has been affected?**	**Transport** ☐ Air transport ☐ Rail transport ☐ Water transport ☐ Road transport **Which essential service has been affected?**	**Health care** ☐ Health care institutions (including hospitals and private clinics) **Which (essential) service has been affected?**
	Energy ☐ Electricity ☐ Petroleum/Oil ☐ Gas	**Banking sector** ☐ Banks **Which essential service**	**Drinking water suppliers and distributors** ☐ Supplier ☐ Distributor **Which essential**

	Which essential service has been affected?	**has been affected?**	**service has been affected?**
	Vital/non-essential ☐ Nuclear ☐ Telecom ☐ Trust services ☐ National government ☐ Water-control structure/management **Which service has been affected?**	**Financial market infrastructure** ☐ Trading platform operator ☐ Central counterparty **Which essential service has been affected?**	**Digital infrastructure** ☐ Internet hubs ☐ DNS suppliers ☐ Register for top-level domain names **Which essential service has been affected?** **As yet unknown** ☐ 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 **wbni@agentschaptelecom.nl**.

Incident notification form for operators of essential services – explanatory notes

Pursuant to the Wbni, any cyber security incident with significant impact on your essential 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.

0.1 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.
How high do you estimate the risk of significant impact?	Complete this field if the incident has not yet had significant impact.
What do you estimate the impact of the damage to be when the significant impact come to pass?	Complete this field if the incident has not yet had significant impact.

0.2 Reporting party information

Must be completed for new notifications.

Company name	The name of the relevant operators of essential services. Use free text to fill in this field.
What type of essential service do you provide?	Indicate the type of essential service you provide, such as electricity, gas or oil/petroleum, or the type of digital infrastructure: TDL, DNS or IX.
Reporting official	Details of the official who reports the incident. Use free text to fill in this field.
Contact official	Details of the contact official. This may be a different person from the one reporting the incident. Use free text to fill in this field.

0.3 Incident information

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

Digital service provider incident with significant impacton the continuity of your essential service	Operators of essential services must also report incidents with significant impacton their essential service that are the result of an incident that took place at a digital service provider whose services they use. This is pursuant to Section 10.3.
Incident nature and scope	Describe the incident. Provide answers to such questions as: which service has been affected and how, at which layer of the organisation did the incident take place, how did

	you establish that an incident had taken place, what are its noticeable consequences, etc. Use free text to fill in this field.This is pursuant to Section 11a.
Suspected date and time the incident began	Indicate the estimated start date and time of the incident. Use the following format when filling in this field dd / mm / yyyy hh: mm (d = day, m = month, y = year, h = hour, m = minute). This is pursuant to Section 11b.
Potential impact of the incident in The Netherlands and abroad	Indicate how this incident will affect other parties within the EU. Try to quantify the impact of the incident in terms of the electricity, gas or petroleum/oil power lost within a specified period. Use free text to fill in this field. This is pursuant to Section 11c.
Estimated recovery time needed	Estimate how much time you will need to close the incident (after notification). This is pursuant to Section 11d.
Description of measures that have been taken to minimise the impact, if any	Indicate which measures you have taken or will be taking to minimise the impact of the incident. These measures may be temporary. Use free text to fill in this field. This is pursuant to Section 11e.
Description of measures that have been taken to prevent the incident recurring, if any	These are the measures you have taken or planned to protect against the incident and its impact permanently and to prevent a repeat of the incident. Use free text to fill in this field. This is pursuant to Section 11e.

1.1 Description of the incident from an ICT perspective

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

Incident category	A security incident may affect one or more of the following factors: – 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. More than one answer may be given.
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?	Indicate what caused the incident, if known. More than one answer may be given. Explain your choice(s).
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.
Incident discovery date and time	Indicate the incident discovery date and time. Use the following format when filling in this field dd / mm / yyyy hh: mm (d = day, m = month, y = year, h = hour, m = minute).
Suspected method of attack	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). 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.

1.2 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. Use free text to fill in this field.

1.3 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 the Cyber Security Incident Response Team for operators of essential services, the NCSC, and the Dutch Data Protection Agency. Use free text to fill in this field.
May Radiocommunications Agency Netherlands share details of your notification with the Cyber Security Incident Response Team for operators of essential services, the National Cyber Security Centre (NCSC)?	Use this field to give Radiocommunications Agency Netherlands permission to share details of your notification with the NCSC.
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.

1.4 Investigation 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.
	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.
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.	

1.5 Other

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

Estimated impact on affected subsectors	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. Under "Which (essential) service has been affected?", indicate which (essential) service in the other subsector has been affected. Use free text to explain the choice.
Incident closure	When closing or withdrawing the incident, indicate the date, time and reason for doing so.