Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy

Form for the **immediate** reporting of security incidents by providers of public electronic communications networks and services

As intended by article 11a.2 first clause of the Dutch Telecommunications Act

This form is intended to inform the Dutch Authority for Digital Infrastructure as soon as possible of security incidents or continuity interruptions. This form and any attachments should then be send to meldplicht@rdi.nl. After the incident is properly evaluated by the notifier a second form containing a finalized and more detailed description of the incident must be sent to the same address within 4 weeks at the latest. Bear in mind that additional information may be requested as a result of this report.

Identification string of the incident |_____

Contact information

Name of the organization |_____

Name of contact person |_____

Telephone number of contact |_____

E-mail address of contact |_____

Incident information

Impact category
(more than one answer possible)

☐ Availability ☐ Authenticity ☐ Confidentiality ☐ Integrity

☐ Impact on redundancy ☐ Threat or vulnerability (Incl. near-miss)

☐ Other: |_____

Which services are impacted?
(more than one answer possible)

NB-ICS

☐ Fixed telephony

☐ Fixed internet

☐ Mobile telephony

☐ Mobile internet

☐ Short Message Service

NI-ICS

☐ Webmail

☐ Voice/Video calls

☐ Text messaging

☐ Conference calls

CONVEANCE OF SIGNALS

☐ Machine-to-machine

☐ Radio distribution

☐ Video distribution

☐ Email (traditional)

EMERGENCY SERVICES

☐ NL-Alert conveyance

☐ 112 conveyance

☐ Satellite services

☐ Other:

Which underlying technology and what (own) brand has been affected?
(e.g. 2g, fiber cables, home subscriber server, encryption elements, stored or sent data, configuration files, malware, user accounts, authentication data, etc.)

What is the (probable) start time of the incident?
(dd-mm-yyyy HH:MM)

date | time

☐ Reliable

☐ Unreliable

What is the (probable) start time of the impact on customers?
(dd-mm-yyyy HH:MM)

date | time

☐ Reliable

☐ Unreliable

What is the (expected) end time of the incident?
(dd-mm-yyyy HH:MM)

date | time

What is the state of the impact of the incident at the time of reporting?

☐ Service has been (mostly) restored

☐ The incident still has an impact on services

☐ Total impact is still unknown

What geographic scale applies to this incident?

☐ Regional   ☐ National   ☐ International

Which region or geographic area is affected?
(end-user perspective)

A description of the situation and the measures taken:
(e.g. cause, solution, (estimated) impact, information supplied to customers, etc.)

☐ Impact on business operations   ☐ Impact on customers

To what extent are services or the network affected? (Including number of affected users, large and small businesses)
(e.g. congestion, interrupted sessions, reduction in quality, information leak, effectiveness of security measures taken, etc.)

Are there any particularities that are deemed relevant?
(e.g. time of expected additional information, feedback on the form, etc.)

Which other parties are involved or informed about this incident?
(where possible provide a brief explanation, for example whether reporting to these or other parties is being considered)

☐ Departementaal Coördinatiecentrum Crisisbeheersing (DCC)   ☐ Autoriteit Persoonsgegevens (AP)

☐ Nationaal Cyber Security Centrum (NCSC)   ☐ Cyber Security Incident Response Team (CSIRT-DSP)

☐ Police (e.g. cybercrime report)   ☐ Veiligheidsregio('s)

Explanation or other parties involved: