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

Form for **completing** a (previously reported) security incident 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 provide the Dutch Authority for Digital Infrastructure with a detailed description of continuity interruptions or breaches of security after internal evaluation of the incident by the notifier has been completed. This form and any attachments must be send to meldplicht@rdi.nl within 4 weeks after the incident has been observed. 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 other parties are involved or informed about this incident?
(provide a brief explanation where possible)

- ☐ Departementaal Coördinatiecentrum Crisisbeheersing (DCC)
- ☐ Autoriteit Persoonsgegevens (AP)
- ☐ Nationaal Cyber Security Centrum (NCSC)
- ☐ Cyber Security Incident Response Team (CSIRT-DSP)
- ☐ Politie (bv. aangifte cybercrime)
- ☐ Veiligheidsregio('s)

Explanation or other parties involved:

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

NB-ICS

- ☐ Fixed telephony
- ☐ Fixed internet
- ☐ Mobile telephony
- ☐ Mobile internet
- ☐ Short Message Service

CONVEANCE OF SIGNALS

- ☐ Machine-to-machine
- ☐ Radio distribution
- ☐ Video distribution
- ☐ Email (traditional)

NI-ICS

- ☐ Webmail
- ☐ Voice/Video calls
- ☐ Text messaging
- ☐ Conference calls

EMERGENCY SERVICES

- ☐ NL-Alert conveyance
- ☐ 112 conveyance
- ☐ Satellite services
- ☐ Other:

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

What geographic scale applies to his incident?

- ☐ Regional
- ☐ National
- ☐ International

Which region or geographic area is affected and what is the approximate size of the affected area?
(end-user perspective)

Please list a timetable of important events concerning this incident:
(dd-mm-yyyy HH:MM, e.g. incident start time, incident start time from the user perspective, incident noticed, incident escalation, service recovery, incident end time, etc.)

How many customers are **potentially** affected?
(break down by service affected, private users, SME & large businesses)

How many customers are **actually** affected?
(break down by service affected, private users, SME & large businesses)

☐ Exact ☐ Reliable ☐ Unreliable

How did the incident proceed chronologically, based on the number of customers actually affected?
(e.g. after one hour, 80% of customers were able to make full use of service X again. The remaining customers had full service recovery two hours after incident start time.)

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

☐ Impact on business operations ☐ Impact on customers

Which sub-providers have been affected?
(Sub-providers are parties that use your infrastructure to provide public communication services)

How was this incident resolved?
(If applicable, differentiate between end of impact for the customer and end of technical failure.)

☐ The incident still has an impact ☐ The impact is not known

What did the information provision for customers look like?

What was the cause and how could this lead to a (partial) failure or breach of the security of your services?

What role did suppliers and external parties play in this incident?
(e.g. cause, effect, solution, etc.)

What (extra) risks do you see as a result of this incident?
(e.g. with regard to own business operations, image damage, financial, with regard to customers; etc..)

Which technical assets were directly affected?
(e.g. mobile base station, international backbone, location registry, UMTS, cabling, Home Subscriber Server, encryption elements, stored or sent data, configuration files, malware, user accounts, authentication data, etc.)

Are there any particularities, or lessons-learned that are deemed relevant in light of this incident?
(e.g. feedback on the form, time of expected additional information, adjustments to work procedures, etc.)