ANCOM
National Authority for Management and Regulation in Communications of Romania

2 Delea Noua Street, Bucharest 3, 030925,Romania
Phone: +40 372 845 400 / +40 372 845 454. Fax: +40 372 845 402
E-mail: ancom@ancom.org.ro. Website: www.ancom.org.ro

On grounds of the provisions of Article 3 letter d), Article 10 paragraph (1) point 1, Article 11 paragraph (1) and Article 12 paragraphs (1) and (3) of Government Emergency Ordinance no. 22/2009 on the establishment of the National Authority for Management and Regulation in Communications, approved by Law no. 113/2010, with the subsequent amendments and completions, as well as of Articles 46 to 48 of Government Emergency Ordinance no. 111/2011 on electronic communications, approved with amendments and completions, by Law no. 140/2012,

THE PRESIDENT OF THE NATIONAL AUTHORITY FOR MANAGEMENT AND REGULATION IN COMMUNICATIONS

issues this:

DECISION

on establishing the minimum security measures to be taken by the providers of public electronic communications networks or of publicly available electronic communications services and on reporting incidents with significant impact on the provision of electronic communications networks and services

Art. 1. – This decision aims to establish:

a) the technical and organisational measures that the providers of public electronic communications networks or of publicly available electronic communications services must take for ensuring an appropriate level of security and integrity of electronic communications networks and services;

b) the circumstances, format and procedures applicable to the notification on the breach of security or loss of integrity with significant impact on the provision of electronic communications networks and services.

Art. 2. – Within the text of this decision, the following terms shall have the following meaning:

1. *security and integrity of electronic communications networks and services* – the ability of an electronic communications network or service to resist accidental events or malicious actions which can compromise or affect the continuity of the provision of networks and services at a performance level equivalent to that preceding the occurrence of the event;

2. *incident* – an event which can directly or indirectly affect or pose threats to the security or integrity of electronic communications networks and services; the effects caused by network maintenance works, scheduled and notified in due time to the users, are not deemed incidents.

3. *incident with significant impact* – an incident which affects more than 5,000 connections for at least 60 minutes;

4. *security measures* – means of risk management (of administrative, managerial, technical or legal nature), including policies, actions, plans, equipment, facilities, procedures, techniques etc. meant to remove or reduce the risks posed to the security and integrity of electronic communications networks or services.

Art. 3. – (1) The providers of public electronic communications networks or of publicly available electronic communications services shall take all appropriate security measures to appropriately manage the risks posed to the security of electronic communications networks and services in order to ensure a level of security appropriate to the identified risk and to prevent or minimise the impact of security incidents on users and interconnected networks, considering the newest technologies and, where applicable, shall collaborate in order to implement these measures.

(2) The providers of public electronic communications networks shall take all appropriate security measures to appropriately manage the risks posed to the integrity of electronic communications networks and services in order to guarantee the integrity of these networks and to ensure the continuity of the provision of services over these networks and, where applicable, shall collaborate in order to implement these measures.

(3) The minimum security measures that the providers should establish and implement in order to comply with the obligations under paragraph (1) and, as applicable, under paragraph (2) shall cover at least the domains identified in annex no. 1.

(4) The providers shall assess and, if necessary, update the measures under paragraph (3) whenever required, but at least once every 12 months.

Art.4. – (1) The providers of public electronic communications networks or of publicly available electronic communications services shall submit to the National Authority for

Management and Regulation in Communications, hereinafter *ANCOM*, a notification on the existence of an incident with significant impact on the security and integrity of electronic communications networks and services.

(2) In enforcing paragraph (1), the providers of public electronic communications networks or of publicly available electronic communications services shall submit to ANCOM an initial notification, no later than 1 p.m. of the working day following the day when the incident with significant impact on the security and integrity of electronic communications networks and services was detected.

(3) The initial notification referred to in paragraph (2) shall be transmitted electronically to the e-mail address incidente@ancom.org.ro by one of the responsible persons according to Article 6, and shall include at least the following elements:

a) time when the incident was detected;

b) services and/or networks affected by the incident;

c) estimation of the affected geographic area, affected number of connections, as well as effects of the incident on the provision of networks and services by other providers, on the national electronic communications market or on the market of another Member State of the European Union;

d) estimation of the impact on the single emergency number (112) calls;

e) a brief description of the cause/causes of the incident;

f) estimation of the schedule for resuming the provision of electronic communications networks and services under normal operation parameters;

g) guidelines offered by the provider to the users for mitigating the effects of the incident, if applicable;

h) information offered to the public regarding the incident, communication means and time when the information was communicated, if applicable;

i) other aspects/elements which may enable ANCOM to decide whether informing the public on the incident is in the public interest;

j) contact data (name and surname, telephone, fax, electronic mail address) of the person/persons who can provide more information on the incident.

(4) The transmission date of the electronic document shall be deemed the date of confirmation by ANCOM of the receipt of the respective document. ANCOM shall ensure without delay and automatically the confirmation of receipt of the electronic document transmitted to the e-mail address incidente@ancom.org.ro.

(5) In the event that the confirmation of receipt of the electronic document was not done under the terms of paragraph (4), the transmission date shall be deemed the date when the electronic document was sent, to the extent this date can be exactly determined.

(6) In enforcing paragraph (1), the providers of public electronic communications networks or of publicly available electronic communications services shall submit to ANCOM a final notification on the existence of an incident with significant impact on the security and integrity of electronic communications networks and services, within two weeks from its detection, by filling out the standard reporting form under annex no. 2, in compliance with the filling out guidelines specified in annex no. 3.

(7) Where, at the time of transmission of the final notification under paragraph (6), the providers do not have available all the information requested in the standard reporting form, they shall send an additional notification with the respective information, by filling out the reporting form under annex no. 2, as soon as this information is available, but no later than 3 weeks from detecting the incident with significant impact.

(8) The final notification and the additional notification referred to in paragraph (6), respectively paragraph (7) shall be transmitted to the ANCOM headquarters in Bucharest or to its territorial offices where the provider's headquarters or domicile are located, in one of the following ways:

a) by submission, personally or through the provider's representative, upon signature;

b) by postal service;

c) in electronic format, by e-mail, to incidente@ancom.org.ro, having included, attached or logically associated an extended electronic signature based upon a qualified certificate that has not been invalidated or revoked at the respective moment, generated by using a secured device for creating the electronic signature.

(9) The submission date is considered, as the case may be, the date of registration in the general registry of incoming-outgoing correspondence of ANCOM, the date of confirmation of receipt of the documents at the ANCOM headquarters by a postal service with confirmation of receipt or the date of confirmation of receipt of the document in electronic format, under the terms of paragraphs (4) and (5).

(10) The standard reporting form under paragraph (6) may be obtained from the ANCOM headquarters or its territorial offices, or from its website.

(11) Starting 1 January 2014, the final notification and the additional notification referred to in paragraph (6), respectively paragraph (7) shall be exclusively transmitted by means of an application available on the ANCOM website as an electronic document having included, attached or logically associated an extended electronic signature based upon a qualified certificate that has not been invalidated or revoked at the respective moment, generated by using a secured device for creating the electronic signature. The provisions of the Decision of the president of the National Authority for Management and Regulation in Communications no. 336/2013 on the means and method of transmission of certain documents, data or information to the National Authority for Management and Regulation in Communications and amending the Decision of the president of

the National Authority for Communications no. 77/2009 on the obligations of informing the end-users, incumbent on the providers of publicly available electronic communications services shall apply as appropriate.

Art.5. – (1) Upon receiving the initial notification referred to in Article 4 paragraph (2) and when deeming it is in the public interest, ANCOM may inform the public on the existence of an incident with significant impact on the security and integrity of electronic communications networks and services, by means of its website, or may require the provider to do so.

(2) At ANCOM's request, the provider of public electronic communications networks or of publicly available electronic communications services shall ensure that the public is informed on the existence of the circumstance described in paragraph (1), using at least one of the following means:

a) a dedicated section on its website;

b) the provider's own television channel;

c) the electronic mail;

d) the short message service;

e) the mass-media.

(3) Where ANCOM did not set alongside the request under paragraph (2) the means and conditions for ensuring the public's information, the provider of public electronic communications networks or of publicly available electronic communications services shall inform the public using at least one of the means described in paragraph (2).

(4) When the significant incident which makes the object of the initial notification under Article 4 paragraph (2) may affect the provision of networks and services by another provider from another Member State of the European Union, based on the gathered information, ANCOM shall decide on informing the regulatory authority from the respective state or the European Network and Information Security Agency, hereinafter *ENISA,* on this incident.

(5) ANCOM shall annually submit a summary report to the European Commission and ENISA on the notifications received pursuant to Article 4 paragraph (6), respectively Article 4 paragraph (7).

Art.6. – The providers of public electronic communications networks or of publicly available electronic communications services shall transmit ANCOM the contact data of the persons in charge of reporting incidents with significant impact on the security and integrity of electronic communications networks and services, within 5 days from the entry into force of this decision, as well as any change in these data, within 5 days from the occurrence of the changes.

Art.7. – Annexes no. 1 to 3 are part of this decision.

Art.8. – (1) This decision shall be published in the Romanian Official Journal, Part One and shall come into force on 1 October 2013, except for the provisions of Article 3 which come into force on 1 January 2014.

(2) The providers of public electronic communications networks or of publicly available electronic communications services shall transmit ANCOM, until 15 October 2013 at the latest, notifications concerning each incident with significant impact on the security and integrity of electronic communications networks and services which occurred in 2013, until the entry into force of this decision, by filling out the reporting standard form provided for in annex no. 2, in compliance with the filling out guidelines under annex no. 3. The provisions of Article 4 paragraphs (8) and (9) shall apply as appropriate.

PRESIDENT,
MARIUS CĂTĂLIN MARINESCU

Bucharest, 1 August 2013
No. 512

ANNEX no. 1

Domains concerned by the minimum security measures

I. Security policy and risk management

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish an adequate security policy;

2) set up a risk management framework that should:

a) define the scope and basic criteria for the risk management process (risk evaluation criteria, impact criteria, risk acceptance criteria);

b) identify risks, by identifying the respective provider's assets, threats, vulnerabilities, the existing measures and the consequences that the loss/breach of security could have on the assets;

c) estimate the risks by assessing the possible impact of a threat that exploits a vulnerability of an asset and by assessing the incident likelihood;

d) evaluate the risk;

e) assess the options available for risk treatment, select risk treatment measures, setting the objectives of these measures and justify the accepted risks that do not meet the risk acceptance criteria;

3) establish an appropriate structure of the roles and responsibilities in ensuring the security and integrity of networks and services;

4) establish a policy regarding the security requirements for procuring products and services from third parties and for ensuring the maintenance or the management of products and services by third parties (IT services, software, interconnection, databases, associated facilities etc.).

II. Human resources security

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) perform background checks on candidates for employment, contractors and third parties in accordance with the applicable laws, regulations and ethics, proportional with the perceived risks;

2) ensure that their personnel have sufficient security knowledge and are provided with regular training regarding the security and integrity of networks and services;

3) establish an appropriate process for managing changes in personnel or changes in their roles and responsibilities;

4) establish a disciplinary process for employees who have committed a breach of security or integrity of electronic communications networks and services.

III. Security and integrity of networks, associated facilities and information

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish an appropriate physical security of the network and of the associated infrastructure (establish and maintain measures that should adequately protect against unauthorised physical access, damages produced by fire, flood, earthquakes, explosion, civil unrest and other forms of natural or man-made disaster);

2) establish appropriate security of supporting facilities, such as electric power, fuel or cooling;

3) establish appropriate security measures for (logical) access to the network and to the information systems;

4) establish appropriate security measures to ensure the protection of electronic communications networks and services against potentially malicious codes, unauthorised mobile codes and cyber attacks, including DoS/DDoS.

IV. Operations management

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish operational procedures and appropriate responsibilities;

2) establish procedures for the management of changes in the electronic communications network and in the application system software;

3) establish asset management procedures in order to verify asset availability and status.

V. Incident management

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish processes and procedures for managing incidents that affect security and integrity of electronic communications networks and services (internal incident reporting, incident assessment, incident response and escalation), including by defining roles and responsibilities;

2) establish an incident detection system;

3) establish an appropriate procedure of incident reporting to the National Authority for Management and Regulation in Communications, as well as to other responsible authorities, and to establish incident communication plans to third parties (affected providers of electronic communications networks and services, media, customers, business partners etc.).

VI. Business continuity management

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish a strategy for ensuring the continuity of the provision of electronic communications networks and services in the event of serious perturbations of the network or service operation;

2) establish capabilities for implementing the continuity strategy and establish continuity and recovery plans.

VII. Monitoring, testing and auditing

Providers of public electronic communications networks or of publicly available electronic communications services have the obligation to:

1) establish policies for system monitoring, as well as logging policies;

2) establish policies for testing, including by exercises, of the continuity and recovery plans in the event of serious perturbations of the network or service operation;

3) establish policies for testing equipment, systems and software, especially before their connection/connecting them to existing systems;

4) establish an appropriate policy for assessing and testing the security of all assets (equipment, systems and software etc.);

5) establish a policy for compliance monitoring and auditing, with a process for reporting compliance and addressing audit deficiencies.

FORM FOR REPORTING INCIDENTS THAT AFFECTED THE SECURITY AND INTEGRITY OF ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES

1. Provider:

2. Date and hour:

2.1 Date and hour when the incident occurred	Date:	Hour:
2.2 Date and hour when the incident was detected	Date:	Hour:

3. Incident impact and cause type:

3.1 Affected service/services:

☐ Publicly available telephone services:
- ☐ provided by means of fixed public networks or networks with limited mobility — Number of affected connections.....
- ☐ by means of public land mobile networks — Number of affected connections.....
- ☐ by means of satellite public networks — Number of affected connections.....
- ☐ call transport services — Number of affected connections.....

☐ leased lines services — Number of affected connections.....

☐ data transmission services (including VPN):
- ☐ at fixed locations — Number of affected connections.....
- ☐ limited mobility — Number of affected connections.....
- ☐ SMS (cellular networks only) — Number of affected connections.....
- ☐ mobile (including MVNO) — Number of affected connections.....

☐ Internet access services:
- ☐ dial-up (local loop only) — Number of affected connections.....
- ☐ permanent connections at fixed locations — Number of affected connections.....
- ☐ mobile radio connections (including MVNO) — Number of affected connections.....

☐ Linear audiovisual media programme retransmission to end-users:
- ☐ fixed or satellite access (DTH type) — Number of affected connections.....
- ☐ mobile or satellite access (S-DAB/DVB-S type) — Number of affected connections.....
- ☐ terrestrial, with access at a fixed location CATV, DVB-C/Mx, IPTV etc. — Number of affected connections.....
- ☐ dedicated terrestrial T-DAB/DVB-T type — Number of affected connections.....
- ☐ public cellular radio (Mobile TV type) — Number of affected connections.....

☐ other electronic communications services
- ☐ professional mobile radiocommunications services
  - ☐ voice — Number of affected connections.....
  - ☐ radio messages — Number of affected connections.....
  - ☐ data transmission, telex — Number of affected connections.....
  - ☐ location, position — Number of affected connections.....
- ☐ other types of services
  - ☐ electronic communications services allowing voice services — Number of affected connections.....
  - ☐ electronic communications services allowing access to content — Number of affected connections.....
  - ☐ other types of services than above — Number of affected connections.....

3.2 Impact parameters:

Total number of connections affected by the incident:

Affected assets/equipment:

Incident duration:

Area/geographic spread:

Impact on emergency calls:

3.3 Incident description:

3.4 Type of incident cause:

- ☐ human error
- ☐ system error
- ☐ natural phenomenon
- ☐ malicious action
- ☐ external cause/third party

3.5 Other information on the incident cause:

4. Other information on the incident

4.1 Incident response actions (including the moment when they were taken):

4.2 Measures taken or planned in order to prevent the occurrence of a similar incident/remove the incident cause (including the moment when they have been/will be taken):
4.3 Other providers of electronic communications networks and services affected:
4.4 Other remarks:

ANNEX no. 3

Instructions for completing the form for reporting incidents that affected the security and integrity of electronic communications networks and services

<table>
<tr><td colspan="2">1. Provider</td></tr>
<tr><td colspan="2">To be filled in with the name of the provider sending the report to ANCOM.</td></tr>
<tr><td colspan="2">2. Date and hour</td></tr>
<tr><td>2.1 Date and hour when the incident occurred</td><td rowspan="2">To be filled in with the date and hour when the incident occurred, respectively when the incident was detected. The format of introducing the date will be dd.mm.yyyy.</td></tr>
<tr><td>2.2 Date and hour when the incident was detected</td></tr>
<tr><td colspan="2">3. Incident impact and cause type</td></tr>
<tr><td colspan="2">3.1 Affected service/services:</td></tr>
<tr><td colspan="2">There will be checked the service/services whose provision was affected by the incident.
The field ”Number of affected connections” for each service type will be filled in accordingly, the number of connections affected by the incident being specified for each affected service.
A connection is:
- for internet access services provided at fixed locations: an internet access connection;
- for data transmission services provided at fixed locations: an access connection to data transmission services;
- for telephone services provided at fixed locations: a telephone line allotted to a subscriber by a provider through its own fixed network or through a third party’s fixed public network; a subscriber may have one or several access lines;
- for telephone services, internet access and data transmission services provided through land mobile networks: an active SIM card;
- for services of retransmission of linear audiovisual media programmes: an audiovisual programme retransmission connection.
For the services provided by means of public land mobile networks, a provider will estimate the number of affected connections. The method of estimating the number of SIM cards affected by an incident is the following:
When an incident occurs, the number of affected cells will be identified.
The total traffic lost for all the affected cells (T_{lost}) for each service (voice and data) will be deemed to be the traffic registered in the previous week, during the same time interval when the incident occurred, for the respective cells.
The total traffic registered on the network ($T_{network}$) is deemed to be the amount of traffic on all the cells of the network within the respective time interval, during the previous week.
The number of affected SIM cards will be calculated as follows:
$$N_{\text{affected SIM cards}} = N_{sd} \frac{T_{lost}}{T_{network}}$$
N_{sd} is the number of active SIM cards for the respective service, according to the reporting based on the Decision of the President of the Authority for Management and Regulation in Communications no. 333/2013 on reporting statistical data by the providers of public electronic communications services or of publicly available electronic communication services.
In calculating the traffic, one takes into account both the originated and the terminated traffic. The proposed algorithm will be applied to all the types of services provided at mobile locations.</td></tr>
<tr><td colspan="2">3.2 Impact parameters:</td></tr>
<tr><td>Total number of connections affected by the incident</td><td>Here will be specified the total number of connections affected by the incident. This number will be calculated as a sum of the number of connections affected for each type of service.</td></tr>
<tr><td>Affected assets/equipment</td><td>There will be specified the assets/equipment affected by the incident. For example, here is a list of the assets that could be affected:
- PLMN base stations (BSC, BTS, RNC, NodeB etc.);</td></tr>
</table>

	- local network (copper wires, fibre etc.); - street cabinets; - switching or routing equipment (networks switches, routers, multiplexers etc.) - transmission nodes; - switching centres; - message centres; - user registers (HLR, VLR, AuC, Home Subscriber Server etc.); - backbone; - interconnections; - equipment for backup supply of electric power (batteries, generators); - power supply systems.
Incident duration	There will be specified the time interval from the moment when the service started degrading or was interrupted, until the moment when it was provided at a performance level equivalent to that preceding the occurrence of the event. Time will be expressed as minutes.
Area/geographic spread	The geographic region affected by the incident will be specified (e.g.: region, counties, localities).
Impact on emergency calls	There will be specified the manner in which communications to the Unique National System for Emergency Calls were affected.
3.3 Incident description:	
There will be provided any information and details available regarding the incident occurrence, development, impact and manner in which the assets/equipment were/was affected.	
3.4 Type of incident cause:	
The incident causes will be checked: human error, system error, natural phenomenon, malicious action and external cause/third party. Usually, the category external cause/third party may be correlated with one of the other 4 causes (e.g.: in the event of a optical fibre destroyed following some construction works, the incident causes will be human error and external cause/third party). Certain incidents may have an initial cause and a subsequent one, incidents being the result of a sequence of events and factors (e.g.: for an incident occurred following a faulty electricity supply – an overload that triggers a breakdown of the provider's equipment, the initial cause is a system error of a utilities provider's equipment and an external cause/third party, while the subsequent cause is a system error – hardware fault of an electronic communications equipment). In this case, the provider will check the initial cause.	
3.5 Other information on the incident cause:	
This field will specify a detailed description of the incident cause, including the exploited vulnerabilities. For the incidents occurred following a sequence of events, the provider will provide both details regarding the initial cause, and the subsequent cause/causes.	
4. Other information on the incident	
4.1 Incident response actions (including the moment when they were taken):	
This field will provide a detailed description of: - the security measures implemented up to the moment of incident occurrence in order to to minimise the incident risk; - actions taken and measures adopted to provide the services at a performance level equivalent to that preceding the occurrence of the event when the incident affects just the service quality (there is no interruption in the service provision); - actions taken and measures adopted in order to bring the service back to a reasonable level, as well as in order to provide the service at a performance level equivalent to that preceding the occurrence of the event in case of interruption of the service provision, including the moments when these were performed.	

4.2 Measures taken or planned in order to prevent the occurrence of a similar incident/remove the incident cause (including the moment when they have been/will be taken):
The field will comprise the detailed description of the actions taken in order to minimize the risk level and to prevent the re-occurrence of the incident (e.g.: review of security measures and procedures, SLA renegotiation, instructing the personnel, backup equipment or systems acquisition etc.), as well as the moment when these measures were or are to be taken.
4.3 Other providers of electronic communications networks and services affected:
This field will be filled in with details about the provider and its assets/services affected by the respective incident, including the cases when providers from another Member States of the European Union were affected. Moreover, the collaboration with other providers for the purpose of solving the incident, including the common incident response actions will be mentioned.
4.4 Other remarks:
This field will be filled in with further details or remarks that were not mentioned in the fields above.