P.I.39/2022

THE SECURITY OF NETWORKS AND INFORMATION SYSTEMS LAW , 2020

Decision under sections 17(j), 17(t), 17(u), 17(x), 17(y), 19(1), 19(2), 20(1)(b), 20(1)(c), 20(1)(d), 20(1)(e), 21, 35(3), 35(4), 35(5), 35(6), 35(7), 35(8), 35(9), 37(3), 37(4), 37(5), 37(6), 37(7), 37(8), 37(9), 37(10), 40(2), 40(3), 40(4), 40(5), 43 and 46

Preamble.

In exercise of the powers vested in it by sections 17(j), 17(t), 17(u), 17(x), 17(y), 19(1), 19(2), 20(1)(b), 20(1)(c), 20(1)(d), 20(1)(e), 21, 35(3), 35(4), 35(5), 35(6), 35(7), 35(8); 35 (9), 37(3), 37(4), 37(5), 37 (6), 37(7), 37(8), 37(9), 37(10), 40(2), 40(3), 40(4), 40(5), 43 and 46 of the Security of Networks and Information Systems Law, 2020, as amended or substituted from time to time, the Digital Security Authority (hereinafter referred to as 'the Authority'), adopts this Decision which prescribes the obligation of operators of essential services, operators of critical information infrastructure, providers of electronic communications networks and/or services and digital service providers to notify any incident that has a serious and/or substantial impact on the continuity of the services they provide.

The Authority adopts this Decision having taken into account, inter alia, the following:

Official Gazette, Suppl.III(I): 12.08.2020.

(a) the provisions of the Security of Networks and Information Systems Law,2020 (L.89(I)/2020),

Official Journal of the EU: L194,19.07.2016, p.1.

(b) the provisions of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common security level of network and information systems across the Union;

Official Journal of the EU: L 321, 17.12.2018, p.36.

(c) the provisions of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018, establishing the European Electronic Communications Code,

Official Gazette, Suppl.III(I): 21.08.2020.

(d) the Security of Information Systems (Security Measures of Operators of Essential Services and Operators of Critical Information Infrastructure) Decision,2020 (P.I. 389/2020),

(e) the National Strategy for the security of networks and information systems and cybersecurity,

(f) the provisions of the ENISA guidelines 2020 on incident notifications related to the establishment of the European Electronic Communications Code;

and by which it prescribes the procedure and content of the notification to be submitted by operators of essential services and/or operators of critical information infrastructure and/or providers of electronic communications networks and/or services and/or digital service providers to the Digital Security Authority for any incident that has a serious and/or substantial impact on the continuity of the services they provide.

PART I
Introductory Provisions

Short title.

1. This Decision may be cited as the Security of Networks and Information Systems (Notification of Incidents) Decision, 2022.

Interpretation.

2.-(1) In this Decision, unless the context otherwise provides;

"Integrity" means maintaining the accuracy and correctness of information;

"Authority" means the Digital Security Authority;

"Authenticity" means ensuring that the source of information and/or services is what it should be;

"Availability" means the continuous operation of services or the ability of access to services or information whenever needed;

"Confidentiality" means access to information only by authorised persons;

"day" means a calendar day, unless otherwise defined in the Law, or unless the context otherwise requires;

"Regulation (EU) 2018/151" means the Commission's Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact;

Official Journal of the EU: L.26, 31.1.2018, p.48.

"incident notification" means the obligation of each operator of essential services, each operator of critical information infrastructure, each provider of electronic communications networks and/or services and each digital service provider to notify the Authority, without undue delay, of incidents which have a serious and/or substantial impact on the services they provide;

"Law" means the Security of Networks and Information Systems Law,2020, and includes any law amending or substituted for the same;

89(I)of2020.

"essential service" means any service which is essential for ensuring the functioning of critical areas of social and economic action, including

essential services and services provided by operators of critical information infrastructure;

"providers of electronic communications" means providers of electronic communications networks and/or providers of electronic communications services;

"providers" means providers of electronic communications and/or digital service providers;

"operator" means the operator of essential services and/or the operator of critical information infrastructure.

(2) Any other terms used in this Decision and not otherwise defined therein shall have the meaning assigned to them by the Law and/or by Directive (EU) 2016/1148 and/or by Directive (EU) 2018/ 1972.

Scope of application of this Decision.

3. This Decision applies to all operators of essential services, operators of critical information infrastructure, providers of electronic communications and digital service providers. This Decision sets out the circumstances under which a security incident has a serious and/or substantial impact on the provision of the services of the above operators and providers, and therefore triggers the obligation of these operators and providers to submit a notification to the Authority. It also regulates the procedure for submitting notifications, in particular the content of notifications, the manner in which they are to be submitted and the deadlines to be respected.

The Authority shall receive the notifications in order to:

(a) manage and respond to incidents which have a serious and/or substantial impact, as defined in paragraph (2) of article 4 and paragraph (5) of article 5 of this Decision;

(b) annually submit to the Cooperation Group and/or ENISA of a summary report on the notifications received, including the number of notifications and the nature of the notified incidents, as well as the follow-up measures taken in accordance with the provisions of the applicable legislation, and

(c) process and analyse notifications for the purpose of a broader assessment of existing security measures taken by operators and providers, with a view to improve the level of security of networks and information systems. The Authority may inform operators and providers of its findings. The data from the notifications may be used to inform competent authorities and to support any planning for enhancing the levels of security of networks and information systems in the Republic of Cyprus:

Provided that the obligations to notify incidents referred to in this Decision concern:

(a) the notifications of incidents at national level and the notifications transmitted to the Authority by any other competent authorities of the member states of the European Union, in accordance with section 17(j) of the Law;

(b) the notifications of incidents which have a serious impact on the continuity of essential services, in accordance with section 17(t) of the Law;

(c) the notifications of incidents, in accordance with section 17(u), 40(2) and 40(3) of the Law, and

(d) notifications of incidents with a substantial impact on the provision of digital services, in accordance with section 17(x) of the Law.

All notifications concern incidents which have an impact on the provision of the above services, resulting from a breach of security of networks and

information systems, or which affect the operation of networks and information systems which are used to provide the aforementioned services.

PART II
MAIN PART

CHAPTER I – NOTIFICATION OF INCIDENTS BY OPERATORS OF ESSENTIAL SERVICES, OPERATORS OF CRITICAL INFORMATION INFRASTRUCTURE, PROVIDERS OF ELECTRONIC COMMUNICATIONS NETWORKS AND/OR SERVICES

Notification of incidents by operators of essential services, operators of critical information infrastructure and of electronic communications providers.

4. -(1) (a) Subject to the provisions of subsection (3) of section 35 of the Law, each operator has a duty to notify to the Authority without undue delay any incident which has a serious impact on the continuity of the essential services it provides.

(b) Subject to the provisions of subsection (2) of section 40 of the Law, each provider of electronic communications has a duty to notify the Authority without undue delay any incident concerning security which had a substantial impact on the operation of electronic communications networks or services.

(2) In accordance with the provisions of ANNEX I – PARTI of this Decision, the significance of the serious and/or substantial impact on the said services which are provided shall be decided by taking into account the following factors:

(a) the number of users affected by the disruption of the essential service;
(b) the duration of the incident;
(c) the geographical scope of the area affected by the incident;
(d) the impact of the incident on health and safety;
(e) the impact of the incident on national security;

(f) the impact of the incident on the economy;
(g) the impact of the incident on social and civil well-being;
(h) the impact of the incident on the natural environment.

(3) The notification must include -

(a) the name of the operator and/or provider of electronic communications and the services it provides;
(b) the time when the incident occurred;
(c) the duration of the incident;
(d) information on the nature and impact of the incident;
(e) information on the likelihood, if any, of the impact of the incident exceeding cross-border limits;
(f) any other information deemed to assist the work of the Authority.

(4) (a) The operator and/or provider of electronic communications must supervise the operation of the information systems and networks supporting the essential services it provides and each time that it detects an incident affecting that function, it shall assess whether the incident has a serious and/or substantial impact, in accordance with the provisions of ANNEX I – PART I. If the incident is considered to have or may have a serious and/or substantial impact, the operator and/or provider of electronic communications shall notify the incident to the Authority.

(b) The initial report shall be provided to the Authority:

(i) without any delay and in any event not later than six (6) hours after the operator and/or provider of electronic communications becomes aware of the incident; and

(ii) in the form set out as ANNEX II to this Decision, by completing all the information required for the initial report :

Provided that, if the incident requires immediate management by the provider and/or the electronic communications provider, and immediate support by the Authority, the operator and/or provider of electronic communications may provide the initial report immediately.

(c) The final report shall be provided to the Authority;

(i) within fifteen (15) days of the restoration of the operation of the affected network or information system; and

(ii) in the form set out as ANNEX II to this Decision, by completing all necessary information:

Provided that, the above timeframes shall not be affected by any actions that the operator and/or provider of electronic communications shall take during its cooperation with the National CSIRT and to prevent future incidents that arise from the management of the incident.

(d) The operator and/or provider of electronic communications is expected to submit an interim report in the event that the information that it has already communicated to the Authority has materially changed or where it is unable to submit a complete final report within the prescribed time limit despite its efforts. The submission of the interim report shall be made by completing as much information as possible in the form set out in ANNEX II to this Decision.

Where the operator and/or provider of electronic communications submits an interim report due to the failure to submit a final report within the timeframe referred to above, the operator and/or provider of electronic communications shall accompany its interim report with a substantiated justification for the delay in submitting the final report, and specify the time of submission of the final report. The interim report shall in no way replace the final one.

(5) The information provided by the operator and/or provider of electronic communications shall be limited to information that it can reasonably be expected to know at the given time.

(6) Upon receipt of the information, the Authority shall assess what further action is needed, if necessary, with regard to the incident.

(7) Upon receipt of such information, the Authority shall inform the competent authorities of a Member State whether the incident has a serious and/or substantial impact on the continuation of the essential service provided in the affected Member State.

(8) Upon receipt of the notification, the Authority shall inform-

(a) the operator and/or provider of electronic communications which provided the information, of any matter related to the incident, including its handling, so that the operator and/or provider of electronic communications can be assisted in handling the incident more effectively and preventing its future recurrence; and

(b) the public about the incident, and/or request the operator and/or provider of electronic communications to inform the public of the incident as soon as possible, where the Authority is of the opinion that it is appropriate for the public to be alert for the purposes of better handling of the incident or to prevent its future recurrence.

(9) Before the Authority informs the public of the incident, or before requesting the operator and/or provider of electronic communications to inform the public of the incident, it shall consult with the operator and/or provider of electronic communications that notified the incident.

(10) The Authority is not obliged to share, as above, the information if:

(a) it contains sensitive or classified information; or

(b) the information is likely to affect the security or commercial interests of the operator and/or provider of electronic communications:

Provided that the final decision to provide information referred to in paragraphs (7), (8) and (9) of this article shall be taken by the Authority.

(11) Without prejudice to the provisions of this article, any operator and/or provider of electronic communications may, on a voluntary basis, notify the Authority of incidents with a less serious and/or substantial impact than that specified in paragraph (2) of this article. For such voluntary notifications of incidents, operators and/or providers of electronic may only submit the information that is mandatory for the initial report as referred to in paragraph (4)(b) of this article.

CHAPTER II - NOTIFICATION OF INCIDENTS BY DIGITAL SERVICE PROVIDERS

Notification of incidents by digital service providers.

5. (1) Subject to the provisions of subsection (5) of section 37 of the Law, every digital service provider has a duty to notify the Authority of any incident which has a substantial impact on the continuity of the services it provides.

(2) The notification obligation applies where the digital service provider has information that enables it to assess whether the incident has a substantial impact.

(3) The information must contain data:

(a) regarding the name of the provider and the services provided;
(b) the time when the incident took place;
(c) regarding the duration of the incident;
(d) regarding the nature and impact of the incident;

(e) regarding the likelihood, if any, of the impact of the incident exceeding cross-border limits; and

(f) other elements which are deemed to assist the work of the Authority.

(4) (a) If the digital service provider considers that an incident has or may have a substantial impact in accordance with the provisions of ANNEX I – PART II of this Decision, the digital service provider shall notify the incident to the Authority.

(b) The initial report shall be provided to the Authority:

(i) without any delay and in any event not later than six (6) hours after the digital service provider becomes aware of the incident; and

(ii) in the form set out as ANNEX II to this Decision, by completing all the information required for the initial report:

Provided that, if the incident requires immediate management by the digital service provider, and immediate support by the Authority, the digital service provider may provide the initial report immediately.

(c) The final report shall be provided to the Authority:

(i) within fifteen (15) days of the restoration of the operation of the affected network or information system; and

(ii) in the form set out as ANNEX II to this Decision, by completing all necessary information.

Provided that, the above time-frames shall not be affected by any actions that the digital service provider shall take during its cooperation with the National CSIRT and to prevent future incidents which arise from the management of the incident.

(d) The digital service provider is expected to submit an interim report where the information that it has already communicated to the Authority has materially changed or where it is unable to submit a complete final report within the set deadline despite its efforts. The submission of the interim report shall be made by completing as much information as possible in the form set out as ANNEX II to this Decision.

Where the provider submits an interim report due to the failure to submit a final report within the timeframe referred to above, the digital service provider shall accompany its interim report with a substantiated justification for the delay in submitting the final report, and specify the time of submission of the final report. The interim report shall in no way replace the final one.

(5) In accordance with the provisions of ANNEX I – PART II of this Decision, the significance of the substantial impact on the above services shall be decided taking into account the following parameters-

(a) the number of users affected by the incident, in particular users who depend on the service in order to provide their own services;

(b) the duration of the incident;

(c) the geographical scope of the area affected by the incident;

(d) the extent of the disruption to the functioning of the service;

(e) the extent of the impact on economic and social activities;

(f) the provisions of article 3 of Regulation (EU) 2018/151.

(6) Where an operator and/or provider of electronic communications relies on a digital service provider, the operator and/or provider of electronic communications, as applicable, shall also notify the Authority of the

substantial impact of the incident on the continuity of the services it provides.

(7) If the notified incident has an impact on one or more member states, the Authority shall inform the competent authorities of the said member states as soon as possible.

(8) The Authority shall not be obliged to share the information as above if the said information.

(a) contains sensitive or classified information; or

(b) may affect the security or commercial interests of a digital service provider.

(9) Upon receipt of the notification, the Authority shall inform:

(a) the digital service provider that provided the information on any matter related to the incident, including its management, so that the digital service provider could in turn assist in the management of the incident more effectively and prevent its future recurrence; and

(b) the public about the incident, and/or request the digital service provider to inform the public of the incident as soon as possible, if the Authority is of the opinion that it is appropriate for the public to be vigilant for the purpose of better managing the incident or to prevent its future recurrence.

(10) The Authority shall inform the public regarding an incident that has a serious impact on the continuity of digital services if:

(a) the competent authorities in the affected Member State have notified the competent authority of the incident;

(b) the Authority has consulted the competent authorities on the matter; and

(c) the Authority is of the opinion that the notification does not adversely affect the security or commercial interests of the digital service provider:

Provided that, the final decision to provide information referred to in paragraphs (7), (8), (9) and (10) of this section shall be taken by the Authority.

(11) Without prejudice to the provisions of this article, any digital service provider may on a voluntary basis notify the Authority of incidents which have a less substantial impact than that specified in paragraph (2) of this article. For voluntary notifications of such incidents, operators may only submit the information that is mandatory for the initial report referred to in paragraph (4)(b) of this article.

PART III
MISCELLANEOUS PROVISIONS

Guidelines for notification purposes.

6. (1) Without prejudice to the provisions of articles 4 and 5 of this Decision, operators and providers must assess whether the incident has a serious and/or substantial impact on the continuity of the services they provide, by taking into account in particular the following parameters:

(a) the number of affected natural or legal persons with whom a contract for the provision of the service has been concluded; or

(b) the number of affected users who have used the service in particular on the basis of previous traffic data and whether the incident has caused

substantial material or non-material damage to users such as in relation to health, safety or property damage; or

(c) the period of time between the disruption of the appropriate provision of the service and the time of restitution; or

(d) the disruption of the operation of the service in terms of the availability, integrity, authenticity or confidentiality of data or related services.

Numbering of incidents, etc.

7. (1) The Authority shall acknowledge receipt of the initial/interim/final notification of an incident no later than one working day after its receipt. In the case of critical incidents, the time to acknowledge receipt of the notification shall be set out in guidelines communicated by the Authority to the operators and providers.

(2) The notifications provided for in this Decision shall be submitted in the form provided in ANNEX II of this Decision. This ANNEX is subject to amendments by the Authority which shall publish the relevant amendment in the Official Gazette of the Republic.

(3) The notifications provided for in this Decision shall be submitted to the Authority electronically, on a dedicated platform that will be operated by the Authority for this purpose. The content of the notification form is set out in ANNEX II to this Decision:

Provided **t**hat, if for any reason, the electronic submission of the respective notification on the dedicated platform is not feasible, then the relevant form shall be submitted to the Authority after the Authority consults with the operators and providers.

(4) The above operators and providers must ensure every time that they submit an initial/interim/final notification in accordance with the provisions of this Decision, that the Authority has received the relevant form that they

have sent. For this reason, in addition to the above, operators and providers must inform the Authority by telephone that they have submitted the form, by contacting the number notified by the Authority.

Clarifications.

8. The Authority may request further information and clarifications regarding the notifications that were submitted if it considers that this is necessary for the fulfilment of its duties. For this reason, operators and providers must retain the relevant information for twenty-four (24) months.

Authorized persons.

9. (1) Operators and providers shall be obliged to notify the Authority of the details of the persons responsible for submitting notifications under this Decision. In particular, operators and providers shall communicate the following details of the persons to the Authority: name, surname, telephone number(s) permanently available (24/7), fax and e-mail address:

Provided that, in case of replacement of the individuals or in case of any change in their data, the operators and providers must immediately inform the Authority.

(2) Operators and providers shall submit to the Authority the information referred to in paragraph (1) of this article within twenty (20) working days of the date of commencement of this Decision.

Administrative penalties.
P.I. 251/2021.

10. Notwithstanding any stricter administrative penalties that may be provided for under the Law, the Authority may impose administrative penalties pursuant to the Collection of Information and Imposition of Administrative Fine Decision, 2021, as amended and/or substituted.

PART IV

Final Provisions

Amendments.

11. The Authority may by Decision amend and/or supplement this Decision and its Annexes. In order to amend or supplement this Decision,

the Authority may carry out a public consultation. Each amendment shall be published in the Official Gazette of the Republic and shall be posted on the Authority's website.

Repeal.

P.I. 371/2013.

P.I.218/2019.

12.From the date of publication of this Decision in the Official Gazette of the Republic, the Notification of Security Breaches or Loss of Integrity of networks and/or services Order of 2013 and the Security of Networks and Information Systems (Notification of Incidents) Decision, 2019, shall be repealed and replaced by this Decision.

Date of commencement.

13.This Decision shall come into effect on the date of its publication in the Official Gazette of the Republic.

ANNEX I – PART I

OPERATORS OF ESSENTIAL SERVICES, CRITICAL INFORMATION INFRASTRUCTURE AND PROVIDERS OF ELECTRONIC COMMUNICATIONS NETWORKS AND/OR SERVICES

In the context of guiding operators of essential services, operators of critical information infrastructure and providers of electronic communications, the following parameters are recorded along with their rationale for the purpose of determining the severity and /or significance of an incident and their impact on the services provided.

In order to judge the severity and/or significance of an incident, it is necessary, firstly, to decide whether the incident is notifiable and, secondly, to highlight its criticality on the basis of the possibility of continuing the service provided or not. Based on the provisions of the current legislation, the following shall be taken into account:

(a) the number of users affected by the incident (excluding loss of life). The number of affected users as a percentage of a country's population is a useful and decisive element for the severity and/or significance of the impact of an incident;

(b) the duration of the incident in the sense of the time elapsed, in minutes or hours, during the time that the incident continues. The duration of an incident determines the extent to which useful areas of social and economic action are affected. The duration of the incident also reveals information about its nature and the possibility of its effective handling. The service provided shall be deemed to have been discontinued until it has been restored and after its confidentiality, integrity, availability and authenticity have been ensured;

(c) the geographical area affected by the incident. The determination of this area highlights the severity and/or significance of the incident on the grounds that the greater geographical area predetermines the severity and/or significance of the impact and whether the incident exceeds cross-border boundaries;

(d) the impact of an incident on safety and health. This parameter aims to determine the users, as a percentage of the population, who are affected by the incident, confirms its severity and/or significance and identifies its priority as a matter of response once it has been notified, and

(e) the extent of the disruption to the service that is provided. This extent highlights the severity and/or significance of the incident and for the purposes of measuring it, the number of individual security objectives that have been affected, such as the confidentiality, integrity, authenticity and availability of the affected service, is taken into account.

The table below sets out the parameters and measurements that constitute the lowest impact levels for notifying an incident to the Authority without undue delay. At the same time, the information provided clarifies the urgency of an incident, its severity and priority and contains all the possible parameters for its overall handling:

Parameter	Measurement	Lower thresholds for notification purposes
When the user-hours of the incident exceed the minimum levels for notification purposes	Calculation of user-hours as the product of the number of affected users multiplied by the duration of the incident in hours.	Every incident where the continuity of the service which is provided by the operator is affected for more than 5000 user-hours. Every incident during which the continuity of service that is provided by a provider of electronic communications is determined to be for more than 20,000 user-hours Continuity of the service is defined as the ability to provide the service at acceptable levels of confidentiality, integrity, availability and authenticity.

Geographical area of an incident if it exceeds the specified minimum limit	Affected administrative/geographical areas	Every incident which as a minimum affects one or more municipal authorities or communities in their entirety.
The impact of an incident on safety and health if it exceeds the lowest thresholds for notification purposes	The number of persons, as a percentage of the population, who have been seriously injured or permanently affected as A result of the essential service that is interrupted by the incident.	Every incident where a minimum of 0.0005% of the population (5 persons) has been seriously injured or permanently affected. In case of death, the incident is automatically subject to notification.
Extent to which an operating service is affected if it exceeds the prescribed notification threshold	The number of individual security objectives (confidentiality, integrity, authenticity, availability) that have been affected by the incident	Any incident which affects one security objective as a minimum. This criterion is expected to be used by Operators of critical information infrastructure (OCII) / Operators of Essential Services (OES) where the impact of the incidents that they face cannot be measured through the remaining criteria.
Whether there are other serious consequences.	YES / NO	Every incident: (1) which had an impact on public alert systems as prescribed by Article 110 of Directive (EU) 2018/1972;

		(2) for which there was an announcement (coverage) in mass media (newspapers, magazines, radio and television) and/or, alternatively, for which an announcement was made on websites and/or in public posts in social media; (3) which caused substantial economic and/or other damage; (4) which caused an impact on important days (e.g. election day); (5) which affected politically exposed persons, as referred to in the Certain Publicly Exposed Persons and Certain Officials of the Republic of Cyprus (Declaration and Control of Property) Law of 2004 (L.50(I)/2004), as from time to time amended and/or substituted, and upon suggestion by the persons themselves that they have been affected by an incident.

Provided that, in cases of incidents that do not meet any benchmark other than the parameter "Whether there are other serious consequences" and as referred to in point 2 under "Lower

thresholds for notification purposes", the deadline of six (6) hours for the submission of the incident applies from the detection of the incident, or is published in Mass Media and/or in Social Media, or indicated by the Authority.

Provided that it is of the utmost importance, in the event of catastrophic incidents, to ensure uninterrupted access to emergency services, such as calls to the number 112 or to national emergency numbers and/or to harmonized numbers for harmonized services of social interest such as the numbers of the series 116xxx, as set out in the Numbering (Electronic Communications) Order of 2018 – P.I. 63/2018, as from time to time amended and/or substituted.

Provided further that, the information to be communicated to the Authority should contain an assessment of any impact on the following:

- The extent of the impact on Public Safety and Public Security, by assessing whether the incident has or may cause a risk to public security and public protection. Upon the notification of the incident, it is up to the Authority to take the appropriate measures with the competent authorities of the Republic of Cyprus, by issuing the necessary instructions to the affected operators and/or providers of electronic communications , where appropriate.

- The extent of the impact on the economy, by assessing whether the incident has or may have actual economic impacts on the same provider and/or provider of electronic communications and/or on other natural and/or legal persons or affect key sectors of economic activity of the country.

- The extent of the impact on social and civil well-being, by assessing whether the incident has or may have a real impact on the quality of social life, on public confidence and orderly living and on the state's ability to ensure social well-being and the standard of living and trust of the public.

- The extent of the impact on the natural environment, by assessing whether the incident has or may have a real impact on natural resources such as water, air and the natural environment.

ANNEX I – PART

DIGITAL SERVICE PROVIDERS

For the purpose of guiding digital service providers, the following parameters are set out which implement the obligation to notify an incident concerning the digital services they provide. For the same purpose, it would be helpful to take into account the following explanations under the parameters on a case-by-case basis:

(a) the number of users affected by the incident; The number of affected users is a useful and decisive element for the importance of an incident's impact.

(b) the duration of the incident in the sense of the time elapsed, in minutes or hours, during the time that the incident continues. The duration of an incident determines the extent to which useful areas of social and economic action are affected. The duration of the incident also reveals information about its nature and the possibility of its effective management. The service provided shall be deemed to have been discontinued until it has been restored and after its confidentiality, integrity, availability and authenticity have been ensured.

(c) the extent of the disruption to the service that is provided. This extent highlights the significance of the incident and for the purposes of measuring it, the number of individual security objectives that have been affected, such as the confidentiality, integrity, authenticity and availability of the affected service, is taken into account.

(d) the extent of the impact, in particular, on matters of national security, public protection, risk of loss of life.

(e) material damage as a result of the incident. The calculation of the material damage caused by the incident highlights the significance of the incident.

The following Table sets out the parameters and measurements that constitute the lowest impact levels for the notification of an incident to the Authority without undue delay:

Parameter	Measurement	Lower thresholds for notification purposes
When the user-hours of the incident exceed the	Calculation of user-hours as the product of the number of	The service provided by a digital service provider was

minimum levels for notification purposes	affected users multiplied by the duration of the incident in hours.	not available for more than 5 000 000 user-hours. The term user-hour refers to the number of affected users in the Union over a period of sixty minutes.
Extent to which an operating service is affected in relation to the number of affected users if it exceeds the specified notification threshold.	Extent of the impact on individual security objectives (confidentiality, integrity, authenticity, availability) that have been affected by the incident in combination with the number of users affected.	The incident resulted in the loss of integrity, authenticity, or confidentiality of stored or transmitted or processed data or related services offered or accessed through a network and information system of the digital service provider, affecting more than 100 000 users within the Union;
Extent of the impact on public safety, public protection or human life.	Assessment of the risk that caused the incident to public safety, public protection or human life.	The incident caused a risk to public safety, public protection, or a risk of loss of life.
Extent of material damage as a result of the incident.	Assessment of the cost of material damage caused by the incident to at least one user.	The incident has caused material damage to at least one user in the Union if the damage caused to that user exceeds 1. 000. 000 EUR

ANNEX II

MODEL INCIDENT NOTIFICATION FORM

This form is intended to be used by operators of essential services ('OES'), operators of critical information infrastructure ('OCII'), providers of electronic communications networks and/or services ('PCNS') and digital service providers ('DSP') for the purpose of notifying incidents, to the Digital Security Authority ('DSA') affecting information systems and networks supporting the essential services they provide. The same form is expected to be used for all three types of reporting identified in the Decision (initial, interim, final). This form can also be used by OES / OCII / PCNS / DSP (or other operators) for the purpose of notifying incidents to the Digital Security Authority on a voluntary basis.

For initial reporting purposes all categories declared as mandatory should be completed, together with any other information available to the reporting operator at the time of submission of the initial report. Where the operator and/or provider of electronic communications networks and/or services and/or the digital service provider cannot fill in accurate data, they must indicate that the information given constitutes an estimate. When a field is not true, it must be marked with "Not Applicable", otherwise the field is considered blank.

Pursuant to paragraphs (2) and (3) of article 7 of this Decision, the content of this form also applies where notifications of cybersecurity and/or digital security incidents are submitted electronically, on a specific platform that will be established for this purpose by the Authority:

Provided that, in the event that for any reason the electronic submission of the notification to this platform is not feasible, then the relevant form shall be submitted to the Authority after consultation of the Authority with the operators of essential services, operators of critical information infrastructure, providers of electronic communications networks and/or services and digital service providers.

In the event that the notification of the incident is submitted electronically, on a dedicated platform to be operated for this purpose by the Authority, the signature provided by the form in this Annex shall be replaced by the addition of a check-box which shall state the following: "I solemnly declare and accept that the information I have entered is correct and I take responsibility for the content of this notification":

Provided that, in case the notification of the incident is submitted electronically, on a dedicated platform to be operated for this purpose by the Authority, operators of essential services, operators of critical information infrastructure, providers of electronic communications and digital service providers will be able to print the notification and at the end of each page of the notification form they must state that "This document is issued automatically by the electronic platform of the Digital Security Authority and is valid without a signature. It was generated from the data that was solemnly declared to the Authority."

NOTIFICATION FORM OF AN INCIDENT TO THE DIGITAL SECURITY AUTHORITY

INTRODUCTORY INFORMATION - (Mandatory for all notifications)

Report by:		Telephone no:	
Title:		E-mail Address:	
Signature:		Report to:	

Type of notification:	Initial	Interim	Final
Notification Type:	Mandatory	Voluntary	

INFORMATION REGARDING THE INCIDENT (MANDATORY FOR ALL NOTIFICATIONS)

Organization Name:		Internal incident number:	
Essential services affected:		Date and time of detection:	
		Date and time of submission of the report :	
Type of incident: (Cybersecurity / Non-Cybersecurity / both)			
Current incident status: (Detected/probable)			
Stage of incident: (In progress/ In progress but under control/ Terminated)			
Essential services that have been affected.			
Number of hours during which the continuity of the			

service was affected (Indicate the number of users and the duration of the incident, in hours)	
Geographical area of an incident	
Were there serious injuries or loss of human life as a result of the incident?	
Extent to which the essential service is affected (confidentiality, integrity, authenticity, availability)	

CYBERSECURITY INCIDENT		Mandatory in the initial notification?
Type of cybersecurity incident:	□ Cyber attack □ System failure	✓

(Cyberattack/ System failure/ Other type - Give details)	□ Other cause	
Main causes:	□ System maintenance / misconfiguration □ System failure □ Software error □ Human Error □ Cyber attack □ Other cause	✓
Secondary cause(If any):	□ System maintenance / misconfiguration □ System failure □ Software error □ Human Error □ Cyber attack □ Other cause	✓
Affected systems: (e.g. servers)		✓
Is assistance from the CSIRT-CY requested? (Please specify your needs) :		✓
ADDITIONAL DETAILS ON THE CYBERATTACK		

Type of attack (If it has been determined):	□ Virus □ Trojan □ Botnet □ DoS / DDoS □ Malware □ Port Scan	□ Spam □Phishing □ Bounce □Pharming □ Probe □ Crack	□ Copyright □Advanced Persistent Threat □Unknown □ Other □ ----------	
Affected systems - Details:* (If these details cannot be specified for the affected system, please provide the necessary information in the General Information section)	IP Address:			
	DNS:			
	Additional Artifacts (MD5, Location, Executable Names, etc.)			
	Operating System:			
Source of the attack (If specified):	IP Address:			
	DNS:			

NON CYBERSECURITY RELATED INCIDENT			Mandatory in the initial notification?
Main cause:	□ Cut cable □ Stolen cable □ Natural disaster (flood, snow, storm) □ Maintenance □ Policy measure/ Procedural system failure	□ Overload □ Physical Attack □ Power surge □ Outage □ Human error □ Other cause	✓
Secondary cause (If any):	□ Cut cable □ Stolen cable □ Natural disaster (flood, snow, storm □ Maintenance □ Policy measure/ Procedural system failure	□ Overload □ Physical Attack □ Power surge □ Outage □ Human error □ Other cause	✓
Affected systems: (e.g. servers, generators, etc.)			✓

INCIDENT DETAILS	Mandatory in the initial notification?

Incident description:		✓
Incident detection: (How was the incident detected?)		✓
Duration of the incident: (indicate start time and full recovery time, if possible)		✓
Is there any known/potential cross-border impact?		✓
Actions taken after the incident was detected:		✓
What other authorities have been informed?		✓
Next steps:		✓
INFORMATION ON THE IMPACT OF THE INCIDENT		
Affected Services/ Systems/ Information that has been affected:		

System Owner / Owner of the Service Provided:		
Administrator of the System/ Infrastructure:		
Impact of the incident(s) on the provision of the service:		
Affected infrastructure assets:		
Other services provided that may have been affected:		
Dependent entities that have been affected:		
Extent of the impact on public safety and public protection (e.g. was there been an impact on public alert systems?)		
Extent of the impact on the economy (e.g. did the incident cause substantial economic or other damage?)		

Extent of the impact on social and political well-being (e.g. 1. the incident caused repercussions on important days such as on an election day, 2. the incident affected politically exposed persons)		
Extent of the impact on the natural environment		
INFORMATION ON THE RESTORATION OF THE SERVICE		
Are BCPs/DRPs enabled? If so, what parts of the relevant plans?		
Time taken to restore:		
KNOWLEDGE GAINED AFTER THE INCIDENT		
Actions to reduce the likelihood of a repetition of the incident or its consequences if it is repeated:		

Lessons (Security measures that could have prevented the incident, additional measures and procedures to be implemented in the long term):		
ANY ADDITIONAL COMMENTS		

Services affected:	□ Fixed telephony (PSTN, ISDN, VOIP, ...) □ Mobile telephony (SMS, 2 G, 3 G, 4 G, 5 G, ...) □ Over the top services (exchange of memos, chats, videos, e-mail, ...) □ Stable internet connection (DSL, satellite, cable) □ Mobile internet connection (GPRS, 2 G, 3 G, 4 G, 5 G, ...) □ Machine-to-machine communication (M2M) (5G, URLCC, MTC) □ Broadcasting television network (TV, radio, ...) □ Other (Please explain): .....
ADDITIONAL INFORMATION *(TO BE COMPLETED ONLY BY PROVIDERS OF ELECTRONIC COMMUNICATIONS NETWORKS AND/OR SERVICES)*	
Description of the main cause of the incident:	□ System failure (software or hardware failure) □ Human Error (human error, oversight) □ Malicious action (cyberattack, physical attack, denial of service attack) □ Natural phenomena □ Failure by a third party □ Other (Please explain) : .....
Additional information (if any):	

Technology affected:	□ Cables □ DSL □ E-mail □ Fiber optics □ GPRS/EDGE □ GSM □ Instant messaging protocol □ LTE □ MTC □ PSTN □ Signal protocol □ UMTC □ URLLC □ VoIP □ Internet/app □ eMBB □ Other (Please explain) : .....
Additional information (if any):	
Causes for the incident	□ Arson □ Cable cutting □ Cable theft □ Failure of cooling systems □ (Distributed) denial of service (DDoS) attack □ Natural disasters (earthquake, flood, snowfall, windstorm, fire, ...) □ Eavesdropping □ Electromagnetic interference

	□ Faulty hardware □ Faulty software □ Lack of fuel □ Hardware failure □ Theft of material □ Identity theft □ Malware / Virus □ Network traffic hijack □ Overload □ Phishing □ Policy/procedure defect □ Power Outage □ Power surge □ Security shutdown □ Software error □ Vulnerability exploit □ Other (Please explain) : .....
Additional information (if any):	

Infrastructure elements affected:	□Addressing server □ Application □ Backup power supplies □ Pricing and mediation systems □ Physical and building security systems □ Cloud storage □ Smart grid devices □ Interconnection points □ Security logic systems □ Mobile base stations and controllers □ Mobile messaging centre □ Mobile switching systems □ Mobile user and location registers □ Operational support systems □ Suspended cables □ PSTN switches □ Power supplies □ SIM/Esim □ Street cabinets □ Undersea cables □ Subscriber equipment □ Routers □ Transmission nodes □ Underground cables □ Web page □ Other (Please explain) : .....
Additional information (if any):	

Other Effects	□ Impact on calls to emergency services, such as, indicatively, calls to the number 112 or to national emergency numbers and/or to harmonized numbers for harmonized services of social interest such as the numbers of the series 116xxx, as these are referred to in the Numbering (Electronic Communications) Order of 2018 – R.A.A. 63/2018, as periodically amended and/or replaced. (Check the box if the availability of emergency services was affected by the incident.) □ Impact on interconnections (Check the box if there were impacts on interconnections that affected other providers in Cyprus or abroad.)
Additional information (if any):	

Explanatory Report

In the context of the new rules which are promoted for cybersecurity, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union was adopted by the European Institutions.

Among the measures taken, a series of collaborations are being developed, at the level of EU member states, in order to minimize cybersecurity incidents to better protect citizens, businesses and public institutions.

By means of the Decision and in the context of the implementation of Directive (EU) 2016/1148, Directive (EU) 2018/1972 as well as sections 17(j), 17(t), 17(u), 17(x), 17(y), 19(1), 19(2), 20(1)(b), 20(1)(c), 20(1)(d), 20(1)(e), 21, 35(3), 35(4), 35(5), 35(6), 35(7), 35(8), 35(9), 37(3), 37(4), 37(5), 37(6), 37(7), 37(8), 37(9), 37(10), 40(2), 40(3), 40(4), 40 (5), 43 and 46 of the Security of Networks and Information Systems Law of 2020, for the purposes of security of networks and information systems, a series of obligations are provided regarding the notification of serious incidents to national authorities by operators of essential services, operators of critical information infrastructure, providers of electronic communications networks and/or services and digital service providers. In particular, the Decision sets out the procedure and content of the notification to be submitted by operators of essential services, operators of critical information infrastructure, providers of electronic communications networks and/or services and digital service providers to the Digital Security Authority for any incident that has a serious and/or substantial impact on the continuity of the services they provide.