P.I. 41/2022

THE SECURITY OF NETWORKS AND INFORMATION SYSTEMS LAW, 2020

Decision under sections 17(r), 17(s), 17(ee), 20(1)(a), 20(1)(b), 20(1)(c), 20(1)(e), 40, 43 and 46

Preamble. 89(I)/2020.	In exercise of the powers vested in it under sections 17(r), 17(s), 17(ee), 20(1)(a), 20(1)(b), 20(1)(c), 20(1)(e), 40, 43 and 46 of the Security of Networks and Information Systems Law, 2020, the Digital Security Authority (hereinafter the''Authority**"),** issues the following Decision establishing the minimum additional obligations regarding the security of networks and information systems to be observed by providers operating electronic communications networks and/or electronic communication services.
Official Journal of the EU: L194,19.7.2016, p.1. Official Journal of the EU: L321,17.12.2018, p.36. Official Gazette, Suppl.III(I): 12.08.2020. Official Gazette, Suppl.III(I): 21.08.2020.	The Authority issues this Decision after taking into account, inter alia: (a) 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 level of security of network and information systems across the Union, (b) the provisions of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code, (c) the provisions of the Security of Networks and Information Systems Law, 2020 (Law 89(I)/2020), (d) decision on the Security of Networks and Information Systems (Security Measures of Operators of Essential Services and of Operators of Critical Information Infrastructure) of 2020 (P.I. 389/2020), (e) the National Strategy for the security of networks and information system and Cybersecurity, (f) the provision of the guidelines of ENISA of 2021 on the security measures related to the establishment of the European Electronic Communications Code.

	PART I **Introductory Provisions**
Short title.	**1.**This Decision may be cited as the Security of Networks and Information Systems (Security Measures of Network and/or Electronic Communications Service Providers) Decision, 2022.
Interpretation.	**2**. (1) In this Decision, unless the context otherwise requires –
	"Network integrity" means the ability provided to an electronic communications network, on the basis of its design, to maintain the functionality for which it is designed and to provide and maintain a high level of service following failures and changes in normal levels of operation;
P.I.389/2020.	"Decision on Security Measures of 2020" means the Security of Networks and Information Systems (Security Measures of Operators of Essential Services and of Operators of Critical Information Infrastructure) Decision of 2020 and includes any decision amending or substituted for the same; "Interconnected networks" means the networks which provide access to each other for the exchange of traffic through, but not limited to, interconnection, leased lines, unbundled local loop access and wholesale broadband access services;
P.I. 63/2018.	"Numbering Order of 2018" means the Numbering (Electronic Communications) Order, 2018 and includes any Order amending or substituted for the same; "guidelines" means the Decisions issued by the Authority pursuant to section 46 of the Law and which aim at clarifying and regulating the procedures, methods and timelines of this Decision;
89(I)/2020.	"Law" means the Security of Networks and Information Systems Law, 2020 and includes any Law amending or substituted for the same;

	«Directive (EU) 2016/1148» means Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union; «Directive (EU) 2018/1972» means Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code; "electronic communications providers" or "providers" means electronic communications network providers and/or electronic communications service providers; "incident" means an incident pursuant t**o** the Security of Networks and Information Systems Law; "emergency plan" means any plan for addressing emergency conditions including the business continuity plan and the disaster recovery plan; (2) Any terms used in this Decision which are not defined otherwise, shall have the meaning assigned to them by the Law and/or the Directive (EU) 2016/1148 and/or the Directive (EU) 2018/1972.
Field of application. P.I. 389/2020.	3. (1) This Decision lays down the minimum additional obligations, beyond the obligations laid down in the Decision on Security Measures, 2020 concerning the security of networks and information that electronic communications providers must comply with.
	(2) The Authority has the ability to issue guidelines for determining the level of implementation of security measures by electronic communications providers: Provided that, the Authority may consult with the providers of electronic communications who have not been designated as operators of essential services and/or operators of critical information infrastructures, for the implementation plan of the security measures required to adopt as it is provided by the Authority's secondary legislation.

Scope.	**4**. The scope of this Decision is to introduce minimum obligations, capable of mitigating the main risks concerning the security of electronic communications providers, so as to ensure the integrity and operational continuity of the networks and services provided to consumers/subscribers in the event of catastrophic damage or in a force majeure event:
P.I. 63/2018.	Provided that, in the case of catastrophic incidents, it is of utmost importance 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 numbers of the 116xxx series, as referred to in the Numbering Order, 2018, as amended and/or substituted for the same**.**
	PART II **Additional obligations of providers of electronic communications**
Governance. P.I. 389/2020.	**5**. In addition to the provisions set out in the “Governance” category in ANNEX III of the Decision on Security Measures of 2020, each provider must also comply with the following obligations.

	(1) To follow the standards or specifications established at Community level which are characterized as mandatory and which have been published in a list of standards or specifications in the Official Journal of the European Communities, for the provision of services, technical interfaces and/or network functions. In case of technical difficulties in complying with the above obligation, the provider shall, within a reasonable time period following an agreement with the Authority, take the necessary measures in order to comply with its obligations mentioned above: Provided that, in the absence of such standards or specifications, the provider is required to apply the latest editions of international standards or recommendations approved by the International Telecommunications Union (ITU), the International Organization for Standardization (ISO) or the International Electrotechnical Commission (IEC). (2)(a) To inform all members of staff of the security policy, which shall be approved by the management and which shall include applicable Laws and Regulations to which the members of staff shall have access. The provider must inform the members of staff about the effects that non-compliance with the security policy may have on their work, (b) To review and, if necessary, update the security policy after security incidents. (3) To ensure that members of staff who hold security roles are accessible in case of security incidents. (4) To inform the members of staff of the competent persons who hold a security role, as well as in what cases the members of staff should communicate with them. (5) To establish operational procedures and to delegate responsibilities to members of staff regarding the operation of critical systems. (6) To implement policy on the operation of systems in order to ensure that all critical systems are operated and managed according to predetermined procedures. (7)To implement a policy and procedures for monitoring and controlling compliance with the relevant legal and regulatory obligations.

Risk management. P.I.389/2020.	**6.** In addition to the provisions set out in the "Risk Management" category in ANNEX III of the Decision on Security Measures of 2020, each provider must also comply with the following obligations: (1) Ensure that key personnel is aware of the main risks as well as the measures for handling them. (2) To review and, if necessary, update the risk assessment following changes (change management) or security incidents.
Awareness and education. P.I.389/2020.	**7**. In addition to the provisions set out in the "Awareness and training" category, in ANNEX III of the Decision on Security Measures of 2020, each provider must also comply with the following obligation: (1) To implement a training program ensuring that all key personnel have adequate and up-to- date security awareness.
Management of third parties and suppliers. P.I. 389/2020.	**8.** In addition to the provisions set out in the "Management of third parties and suppliers", category, in ANNEX III of the Decision on Security Measures of 2020, each provider must also comply with the following obligations: (1) (a) To define a security policy for contracts with third parties, in order to ensure that any dependencies thereon shall not negatively affect the security of its networks and/or services. At a minimum, the policy should include provisions for confidentiality as well as for the secure exchange of information, (b) To ensure that all supply of services or products from third parties follows the third party contract security policy, (c) To review and, if necessary, to update the security policy of contracts with third parties following security incidents or changes, (d) To require, for the duration of the supply, the use of specific security standards in the supplier's procedures, (e) To limit residual risks which are not addressed by third parties.

Management of changes. P.I. 389/2020	**9.** In addition to the provisions set out in the "Change Management" category, in ANNEX III of the Decision on Security Measures of 2020, each provider must also comply with the following obligations: (1) To apply change management procedures and to record the steps of the procedure followed for each change. (2) The providers must at all times keep available backup copies of the most recent configuration of their network equipment which are necessary for the restoration of their network and the services provided. Backups should be kept at a secure location. (3) The providers must have change management procedures which they must apply in cases where changes occur (indicatively, organizational changes, software or hardware changes), which could in any way affect the network or the availability of the services provided: Provided that, any changes should be made in such a way so as to cause the least possible impact on the operation of the network, on the services provided and on other cooperating providers. If these changes inevitably affect another provider's networks or services, the parties involved must work together in order to manage the changes so as to minimize any impact.

Asset management. P.I. 389/2020.	**10.** In addition to the provisions set out in the "Asset management" category, in ANNEX III of the Decision on Security Measures ,2020, each provider must also comply with the following obligations: (1) To follow best practices for the use of encryption algorithms and the encryption keys to be used shall have the recommended size depending on the algorithm that is used. (2) (a) To ensure that cryptographic material, such as keys and secret authentication information are not disclosed nor tampered with; (b) To control in a strict manner and to monitor access to private keys. (3) To implement a policy for the management of cryptographic keys. (4) (a) To implement a policy for monitoring critical systems and maintaining log files; (b) To use tools for the collection and storage of log files on an independent server. (5) (a) To carry out preventive maintenance works on its equipment, as well as at the buildings in which it is located, on the basis of a predetermined time schedule that is prescribed either by the manufacturer of the equipment or by the internal procedures of the provider, in order to minimize the possibility of malfunction of the network and of the services provided: Provided that, to the extent possible, network maintenance works should be carried out without interrupting the network or the services provided, (b) In the case of planned maintenance works, the provider shall have an obligation to inform its associates – providers (in the case of interconnected networks) as well as subscribers/users of the network's services who may be affected by the scheduled interruption in advance within a reasonable period of time. The provider must inform the subscribers/users of the network's services who may be affected by the planned interruption as prescribed by article 21(1) of this Decision.

Management of identity and access. P.I. 389/2020.	**11.** In addition to the provisions set out in the "Management of identity and access" category, in ANNEX III of the Decision on Security Measures of 2020, each provider must also comply with the following obligations: (1) To strengthen controls for remote access at critical network and information system assets by third parties: Provided that, remote access to critical assets by third parties must be granted upon reasonable cause and must be subject to strict access controls, including authentication and authorization controls, especially for privileged accounts. (2) To implement a policy for managing user passwords.
Network Security. P.I.389/2020.	**12**. In addition to the provisions set out in the "Network Security" category, in ANNEX III of the Decision on Security Measures of 2020, each provider must also comply with the following obligations: (1) (a) To ensure appropriate backup of critical elements of its network, so that any possible damage does not cause a significant alteration of the operation of the network and of the services provided to its subscribers, (b) To plan backup solutions in parts of its network, with the backup reflecting the criticality of the parts of the network based on the outcome of the risk assessment of the network that it has previously carried out: Provided **t**hat the design of the network should provide for the implementation of automatic backup solutions that allow the uninterrupted operation of the network. In cases where it is not technically possible to implement the planning of automatic backup solutions (automatic routing of traffic through alternative routes), then the provider must take the necessary actions to quickly repair the fault,

	(c) To design its networks so that the redundancy of the critical elements of the networks is achieved in a way that allows the installation of the critical elements in different premises of the provider, in a way that ensures redundancy through geographical dispersion. The provider may refrain from this obligation when objective reasons impose a different design of its network. In any case, the provider must inform the Authority of the reasons for this inability in order to assess its reliability and impose proportional obligations.
Security of systems. P.I. 389/2020.	**13.** In addition to the provisions set out in the "Security of systems" category, in ANNEX III of the Decision on Security Measures, 2020, each provider must also comply with the following obligation: (1) To implement enhanced measures for software integrity and the management of security updates for critical assets in virtualized networks.
Physical security. P.I. 389/2020.	**14.** In addition to the provisions set out in the "Physical security" category, in ANNEX III of the Decision on Security Measures, 2020, each provider must also comply with the following obligations: (1) (a) to implement a policy of physical security measures and environmental controls, including on the facilities and systems which are covered; (b) to implement enhanced measures for physical access to critical assets: Provided that, physical access to critical assets should be controlled and should be provided only to a limited number of trained and specialized personnel. Access by third parties is only permitted if there is a reasonable cause and must be controlled and must be controlled and monitored.

	(2) To ensure the security of critical supplies. The provider must inter alia have a backup power supply and/or backup fuel. (3)(a) To implement a policy for the security of critical supplies; (b) To implement high-level security measures in order to protect critical supplies and support facilities: Provided that, high-level security measures include, inter alia, automatic restart following a power outage, backup batteries, generators and backup fuel.
P.I. 247/2013.	(4) To ensure the physical security of facilities where its network equipment is installed by taking physical security measures for each building according to the critical nature of the equipment that it is hosting. In case of co-location, the distribution of responsibility for the physical security of the facilities as well as for controlling access shall be carried out under the relevant framework agreement between the parties, in accordance with article 9(1)(d) of the Provision of Co-location and Shared Facilities Order, 2012, as amended and/or substituted for the time being. Indicative physical security measures include property access control, protection against earthquakes, floods, overheating, fire, lightning and other natural disasters.

	(5) To follow plans that guarantee that the elements of the network and/or services, which have been evaluated as vital, are installed in different facilities or in physically independent spaces. In cases where the network elements cannot be installed in different premises, provision should be made for the equipment to be protected by independent means of physical protection. (6) With regard to the control of access to premises where network equipment is installed that have previously been characterized as vital, special systems should be installed to prevent unauthorized access and security procedures should be established through which access is controlled to the spaces mentioned above. (7) To have mechanisms and procedures in order to immediately be informed of incidents which threaten the physical security of the elements of the network and of the premises in which they are installed. (8) To cooperate with competent entities and services (state and private owned), with the aim of minimizing the possibility of causing damage to the elements of the network and/or its service, in cases where works carried out that may affect its network.

	(9) (a) To ensure that the main power supply of the equipment is provided on the basis of its appropriate specifications, (b) To ensure the uninterrupted supply of power in case of interruption of the main power supply in a building where the critical points of the network are located due to a failure, (c) To ensure that the supply of power to the critical elements of the network is not interrupted in case of interruption of the main power supply, (d) Common practices applied in cases of loss of the main power source are included in ANNEX 3 of this Decision. (10) To take all necessary measures for adequately protecting the equipment used in its networks:

	Provided that the protection of equipment concerns in particular the observance of measures for the physical protection of the equipment, the observance of the operating specifications of the equipment as well as the observance of its maintenance requirements: Provided further that, in case it is established that a component of equipment or of a network causes a degradation of the network's operational capacity, the providers must immediately take measures to restore the orderly operation of the network, restoring the normal operation of the equipment as soon as possible or disconnecting it from the network as a measure of last resort.

Management of incidents and events. P.I.389/2020 .	**15.** In addition to the provisions set out in the "Management of incidents" category, in ANNEX III of the Decision on Security Measures, 2020, each provider must also comply with the following obligations: (1) to ensure that its members of staff is available and ready to handle security incidents. (2) to use effective systems and procedures in order to detect security incidents.

Business continuity and resilience. P.I.389/2020.	**16.** In addition to the provisions set out in the "Business continuity and resilience" category, in ANNEX III of the Decision on Security Measures of 2020, each provider must also comply with the following obligations: **(1)** (a) To monitor the activation and execution of the emergency plans and to record the successful and unsuccessful times of recovery of the network and/or of the services provided, (b) To ensure that emergency plans include provisions for dependent and interdependent to operators of essential services and/or operators of critical information infrastructure. **(2)** To ensure the existence of a high level of disaster recovery capabilities or that they are available from third parties. **(3)** (a) To implement an exercise program for testing contingency plans and for recovering data backups at regular intervals by using realistic scenarios, which will cover a range of different scenarios over time; (b) To ensure that the lessons learned from the exercises are taken into account by those persons who are responsible for the appropriate updating of procedures and systems. **(4)** To take the necessary measures to ensure uninterrupted access to emergency services. Indicative measures include the alternative routing of calls, the avoidance of single points of failure, such as the avoidance of dependence on machinery installed in one place for managing calls to emergency numbers and the existence of channels dedicated exclusively to emergency numbers: Provided that, the provider must ensure the priority of calls made to emergency services:

P.I. 63/2018.	Provided further that, in the case of catastrophic incidents, it is of utmost importance to ensure uninterrupted access to emergency services, such as calls to the number 112 or to national emergency numbers or to harmonized numbers for harmonized services of social interest such as the series numbers 116xxx, as set out in the Numbering Order of 2018, as amended and/or substituted for the same.
Other measures.	**17.** In addition to the obligations set out in this Decision, each provider must also comply with the following obligations: (1) To carry out tests on networks and information systems, before using them or connecting them to existing systems. (2) (a) To implement a policy and procedures for testing network and information systems; (b) To implement tools for automated testing. (3) To be regularly informed on cyber threats by monitoring external threat intelligence flows and by exchanging information with relevant Organizations. (4) To implement a program for the collection and sharing of information on cyber threats (threat intelligence program), which should include, inter alia, the definition of the roles, responsibilities and related procedures.

Network Management System.	**18.** (1) Each provider must monitor the status of its network components/equipment continuously and in real time through the operation of an appropriate Network Management System, in terms of their operational capability and possible faults which may occur during the operation of the equipment. Every provider must also consider the possibility of creating a Security Operations Centre for better monitoring network security issues and (2) Every provider must maintain staff who shall work on a shift schedule, so that they can immediately respond to breakdowns that may affect the services provided to subscribers.
Management of traffic growth.	**19.** (1) Every provider must protect the integrity of its network from conditions of increased traffic, using traffic management techniques with the aim of timely detecting increased traffic and protecting the network therefrom. **(2)** Every provider must scale its network according to the forecasts that it carries out for incidents that may cause a significant increase in traffic on its network. **(3)** Every provider must prioritize the calls of operators of basic services and/or operators of critical information infrastructures in cases of emergency, upon the request of such operators. **(4)** Every provider must record the traffic management techniques and the conditions under which they apply the same. It must also record the measures that it uses in order to ensure the prioritising of traffic to the emergency services, particularly in emergency situations.

PART III

Provision of information

Mutual information of providers.	**20.** (1) Every provider must inform in a timely manner as well as in writing and through agreed channels the providers of other networks that may be affected by planned works on their network, including maintenance works. **(2)** Each provider must notify the providers of other interconnected networks in a timely and appropriate manner of expected incidents that may cause particularly increased traffic on its network and which may affect the networks of other providers. **(3)** In the case of interconnected networks, the provider who perceives an error must immediately notify other providers who may be affected thereby. The provider must take immediate measures to repair the damage. **(4)** Providers that interconnect their networks should have clear and recorded communication procedures available between their staff and the staff of the providers of interconnected networks, in order to cooperate and coordinate the procedures for restoring the smooth operation of networks: Provided that, the manner of communicating / exchanging informational messages between providers shall be described in specialized agreements between the two Parties.
Consumer information.	**21. (**1) Every provider must, where possible and in case the network is unable to process telephone calls for a period of at least one (1) hour due to a breakdown or due to planned maintenance works and in cases of outages that will exceed a duration of at least one (1) hour, inform the subscriber/user by a recorded message concerning the inability to provide the service as well as the subscribers/users of the network services who may be affected by the planned interruption. The recorded message shall be transmitted when the subscriber/user attempts to make a telephone call. In any event, the provider's staff must be sufficiently up- to -date so as to provide the relevant information at the consumer's request:

P.I. 63/2018.	Provided that, in cases where the network is unable to process telephone calls due to a breakdown or due to scheduled maintenance works, subscribers/users of the network services who may be affected by the breakdown or planned outage are informed by providing a recorded message and/or by sending a text message(sms) and/or by sending an email to the affected subscriber/user: Provided further that, the subscribers/users of network services who may be affected by the planned outage, must also be informed by means of an announcement on the provider's official website by a public post on the provider's official social media accounts and/or by announcement in mass media: Provided even further that, in cases where it is known that a communication method cannot work as mentioned above, then the provider shall have an obligation to use the corresponding means in order to inform the consumers/users of its network services in a manner that ensures the completion of this information: Provided even further that notification must be immediate where access to emergency services is affected, 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 116xxx series, as these are set out in the Numbering Order, 2018, as amended and/or substituted for the same. (2) Every provider must implement a policy and procedures in order to regularly inform end-users on security threats to networks and/or services that may affect them.

	PART IV **Control and consultations**
Control and evaluation of information. P.I.389/2020.	**22.** The Authority may at its discretion check the correct implementation of the obligations arising under this Decision and the relevant Annexes, as well as the accuracy of the information provided to it in accordance with this Decision by applying the provisions of article 16 of PART VIII of the Decision on Security Measures, 2020: Provided that the documents imposed by article 13 of the Decision on Security Measures, 2020 under which every provider is obliged to provide the relevant information to the Authority, shall also cover the additional obligations included in this Decision.
Public Consultations. P.I. 389/2020.	**23**. Subject to the provisions of article 17 of PART VIII of the Decision on Security Measures, 2020, the Authority may, if it considers necessary, consult with the interested parties on a case-by-case basis regarding matters of security of networks and information systems.
,	**PART V** **Compliance - penalties**
Breach of obligation. P.I.389/2020.	**24.** If a provider breaches an obligation arising from this Decision, the provisions of PART IX of the Decision on Security Measures ,2020 shall apply.
	PART VI **Final Provisions**
Compliance with the action plan. P.I. 389/2020.	**25**. In order to implement the provisions of this Decision every provider must comply with the action plan provided for in article 21 (1) (b), (c) and (d) of the Decision on Security Measures ,2020. In exceptional cases, following a reasoned request from the provider of electronic communications networks and/or services and if this is objectively justified, the Authority may accept an appropriate adjustment of the compliance deadlines for each individual case.

Amendments.	**26.** The Authority may by its Decision repeal/replace, amend and/or supplement this Decision and/or its Annexes. In order to amend or supplement this Decision and/or its Annexes, 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 website of the Authority.
Repeal. P.I. 253/2011.	**27**. Three (3) months from the date of publication of this Decision in the Official Gazette of the Republic, the Network and Information Security Order,2011 shall be repealed and replaced by this Decision.
Date of commencement.	**28.** This Decision shall come into effect within three (3) months from the date of its publication in the Official Gazette of the Republic.

ANNEX 1: RISK ASSESSMENT FRAMEWORK

In addition to the provisions of ANNEX I of the Decision on Security Measures, 2020 (P.I. 389/2020), in the context of risk assessment, each provider must also comply with the following:

As a best practice, providers are encouraged to define criteria/parameters based on which their network elements shall be prioritized, in terms of their criticality/importance, with respect to the operation of the network and the availability of service. The prioritization of the importance of the network components shall significantly affect the adoption of corrective measures.

In the context of the interconnection of networks of one or more providers, providers should also record the connection of the critical components of their network to other networks.

ANNEX 2: BUSINESS CONTINUITY PLAN

In addition to the provisions of ANNEX I of the Decision on Security Measures ,2020 (P.I. 389/2020), the business continuity plan of each electronic communications provider should include:

The recovery times in different damage conditions. In cases of damage due to a third-party network (where the provider's network is hosted on the premises of another network), the

provisions included in the relevant agreements concluded on the basis of Service Offer Models, as amended by the Commissioner, shall apply.

ANNEX 3: COMMON PRACTICES FOR DEALING WITH LOSS OF POWER SUPPLY

(1) Common practices applied by electronic communications providers, in cases of loss of the main power source of the premises/web etc., consist of the existence of backup batteries that can support the operation of the equipment for a short period of time, as well as generators.

(2) Backup batteries should have sufficient capacity to support the operation of critical network components from the moment of interruption of the power supply to the public power network until the commencement of operation of the generators. Backup batteries shall be maintained according to the manufacturer's conditions and all measures shall be taken to ensure their proper operation.

(3) The time for which the continuity of operation of the network components is ensured through backup supply shall differ for each network element and planning shall always be made on the basis of the outcome of the risk assessment and the identification of the critical components of the provider's network.

(4) Furthermore, each electronic communications provider should ensure that there is a sufficient number of backup portable generators to service its network and is encouraged to have an additional source of backup power for critical components of its network which are not served from the same source.

(5) Each provider should carry out regular checks to ascertain the operational level of the back-up power systems at all times, including procedures for supplying fuel to the generators.

EXPLANATORY STATEMENT

According to sections 17(r), 17(s), 17(ee), 20(1)(a), 20(1)(b), 20(1)(c), 20(1)(e), 40, 43 and 46 of the Security of Networks and Information Systems Law,2020, the Digital Security Authority issues a Decision on the Security Measures of Network and/or Electronic Communications Service Providers.

The Decision defines the minimum additional obligations regarding the security of networks and information systems, beyond those defined in the Decision on Security Measures, 2020 (P.I.389/2020) as amended and/or substituted for the time being, which must be observed by electronic communications providers which operate electronic communications networks and/or services.