EnCaViBS

WP 2: The NIS Directive and its transposition into national law.

Member State:

France

Order of 14 September 2018 setting out the security rules and time frames referred to in Article 10 of Decree No. 2018-384 of 23 May 2018 on the security of networks and information systems of operators of critical services and digital service providers

Important notice:

This text is an unofficial translation conducted at the SnT/ University of Luxembourg in the framework of the research project EnCaViBS.

The original legal acts which Member States notified to the European Commission as national execution measures were retrieved from official national databases. In order to focus on the core of the research project, only selected transpositions have been translated.

The translations only serve the purpose of being an information resource; there is no guarantee whatsoever that the translations correctly correspond to the original versions of the laws. Therefore, evidently, the texts have no legal value. The original, as well as the translated version of the legal acts, are available at www.encavibs.uni.lu, where additional information on the research project may be found.

This research project is funded by the Luxembourg National Research Fund (FNR), C18/IS/12639666/EnCaViBS/Cole,

https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Fonds National de la Recherche Luxembourg

Member State: France

Order of 14 September 2018 setting out the security rules and time frames referred to in Article 10 of Decree No. 2018-384 of 23 May 2018 on the security of networks and information systems of operators of critical services and digital service providers

JORF no. 0225 of 29 September 2018

The Prime Minister,

Having regard to 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;

Having regard to the Defence Code, in particular Articles L. 2321-1, R. * 1132-3 and R. 2321-1;

Having regard to the General Code of Territorial Communities, in particular Article L. 1212-2;

Having regard to the Monetary and Financial Code, in particular Article L. 614-2;

Having regard to the Mutual Code, in particular Article L. 411-1;

Having regard to Act No. 2018-133 of 26 February 2018 containing various provisions for adapting to European Union law in the field of security, in particular article 6 thereof;

Having regard to Decree No. 2009-834 of 7 July 2009, as amended, creating a department with a national remit known as the "National Agency for information systems security";

Having regard to Decree No. 2015-350 of 27 March 2015, as amended, on the qualification of security products and trust service providers for the purposes of information system security;

Having regard to order no. 2018-384 of 23 May 2018 on the security of the networks and information systems of operators of critical services and digital service providers, particularly its article 10;

Having regard to the opinion of the National Standards Assessment Board dated 13 September 2018;

Having regard to the opinion of the Advisory Committee on Financial Legislation and Regulation dated 12 July 2018;

Having regard to the opinion of the Conseil supérieur de la mutualité dated 12 July 2018,

Orders:

Article 1

The security rules mentioned in Article 10 of the aforementioned Decree No. 2018-384 of 23 May 2018 are set out in Appendix I to this Order. Operators of critical services shall apply these security rules to the networks and information systems mentioned in Article 7 of the aforementioned decree, from he date of their designation as operators of critical services within the timeframes set out in Appendix II of this Order.

Article 2

This Order shall apply throughout the Republic.

Article 3

This order comes into effect on 1 October 2018.

Article 4

This order shall be published in the Official Gazette of the French Republic.

APPENDICES

Appendix I

Security rules

These security rules are applicable to the networks and information systems mentioned in Article 7 of Decree No. 2018-384 of 23 May 2018 on the security of networks and information systems of operators of critical services and digital service providers. These networks and information systems are referred to in this Annex as "critical information systems".

Chapter I: Rules relating to the governance of network and information system security

Rule 1. Risk analysis

The critical service operator shall perform and maintain, within the framework of the security accreditation provided for in Rule 3, a risk analysis of its critical information systems (CIS). This risk analysis shall consider the analysis that the operator has conducted to identify its information systems as CIS.

Rule 2. Security policy

The operator of critical services shall develop, maintain and implement a network and information systems security policy (NISSP). The NISSP describes all the organisational and technical procedures and resources deployed by the operator to ensure the security of its critical information systems (CIS). In the area of security governance, the NISSP defines:

- the strategic objectives and directions in matters of CIS security;

- the organisation of security governance, including the roles and responsibilities of internal staff and external staff (contractors, suppliers, etc.) with respect to CIS security;

- CIS security awareness plans for all staff as well as CIS security training plans for individuals with specific responsibilities, including those responsible for CIS administration and security and users with special access rights to CIS;

- the CIS security certification procedure;

- CIS security control and audit procedures, including those deployed in the framework of security accreditation.

In the area of protection, the NISSP defines:

- general security measures, including the management and security of CIS hardware and software resources, control of access to CIS, the operation and administration of CIS, and network, desktop and data security;

- physical and environmental security procedures and measures applicable to CIS;

- the procedure for keeping CIS resources secure.

In the field of defence, the NISSP defines:

- the procedure for detecting security incidents;

- the procedure for handling security incidents.

In the area of business resiliency, the NISSP defines:

- the crisis management procedure in the event of security incidents having a major impact on the operator's critical services;

- Business continuity and recovery procedures.

The NISSP and its implementing documents are formally approved by the operator's management. The operator prepares a report on the deployment of the NISSP and its implementation documents for the benefit of its management, at least annually. This report mainly focuses on the inventory of risks, the level of security of the CIS and the security actions carried out and planned. The operator shall keep the NISSP, its implementing documents and the reports on their implementation available to the National Agency for information systems security.

Rule 3. Security certification

The operator of critical services shall ensure the security certification of each critical information system (CIS), by implementing the certification procedure provided for in its network and information systems security policy. The certification of a system is a formal decision by the operator that the system's security risks have been identified and that the necessary measures to protect the system have been implemented. It also certifies that any residual risks have been identified and accepted by the operator. Within the framework of the certification process, a security audit of the CIS shall be carried out in accordance with rule 5. The operator makes the decision to approve a CIS on the basis of the certification file, which includes:

- the analysis of the risks and security objectives of the CIS;

- the procedures and security measures applied to the CIS;

- CIS security audit reports;

- the residual risks and the reasons for accepting them.

The validity of the certification shall be reviewed by the operator at least every three years and at the time of each event or development which alters the context described in the certification file. Each review of the certification is recorded in the certification file. The operator renews the approval as soon as it becomes invalid. The operator shall make the certification decisions and files available to the National Agency for information systems security.

Rule 4. Indicators

The critical service operator shall assess and maintain the following indicators for each critical information system (CIS):

- Indicators for keeping resources secure:

- the percentage of user work stations whose system resources are not installed in a version supported by the vendor or manufacturer;

- the percentage of servers whose system resources are not installed in a version supported by the vendor or manufacturer;

- indicators relating to user access rights and the authentication of access to resources:

- the percentage of users accessing the CIS through privileged accounts;

- the percentage of resources whose secret authentication elements cannot be changed by the operator;

- indicators related to the administration of resources:

- the percentage of administered resources that are administered from a non-specific administration account;

- the percentage of administered resources that cannot be administered over a physical network link or physical administration interface.

The operator shall specify for each indicator the assessment method used and, as applicable, the margin of uncertainty in its assessment. When an indicator changes significantly compared to the previous assessment, the operator shall specify the reasons thereof. The operator shall provide the National Agency for the Security of Information Systems, at its request, with the updated indicators on an electronic medium.

Rule 5. Security audits

The essential service operator shall, within the framework of the security certification under Rule 3, carry out a security audit of each critical information system (CIS). The audit must also be carried out at the time of each renewal of the certification, considering the results of the updated risk analysis of the CIS.

The purpose of this audit is to verify the application and effectiveness of the CIS security measures and particularly compliance with these security rules. It must enable the level of security of the CIS to be assessed in terms of known threats and vulnerabilities and includes, in particular, an architecture audit, a configuration audit and an organisational and physical audit.

The operator or the service provider approved for this purpose shall carry out this audit based on the requirements of the reference framework for security audits of information systems adopted pursuant to Article 10 of Decree No. 2015-350 of 27 March 2015, as amended, relating to the classification of security products and trusted service providers for information system security purposes. Upon completion of the audit, the operator or, as applicable, the service provider, shall draw up an audit report setting out the findings on the measures applied and compliance with these security rules. The report shall state whether the level of security achieved is consistent with the security objectives, considering known threats and vulnerabilities. It makes recommendations to deal with any non-compliances and vulnerabilities found.

Rule 6. Mapping

The operator of critical services shall develop and maintain the following mapping elements for each critical information system (CIS):

- the names and functions of the applications supporting the operator's activities and installed on the CIS;

- as applicable, the IP address ranges for outputs from the CIS to the Internet or a third party network, or accessible from these networks;

- as applicable, the IP address ranges associated with the various subnets making up the CIS;

- the functional description and installation locations of the CIS and its various sub-networks;

- a functional description of the interconnection points of the CIS and its various sub-networks with third-party networks, including a description of the filtering and protection equipment and functions deployed at these interconnections;

- the inventory and architecture of the CIS administration devices enabling remote installation, updating, supervision, configuration management, authentication and the management of accounts and access rights;

- the list of accounts with privileged access rights to the EIS (called "privileged accounts"). This list specifies for the level and scope of associated access rights for each account, including the accounts to which these rights apply (user accounts, email accounts, process accounts, etc.);

- the inventory, architecture and positioning of host name resolution, messaging, internet relay and remote access services implemented by the CIS.

The operator shall provide the National Agency for the Security of Information Systems, at its request, with the mapping elements updated on an electronic medium.

Chapter II: Rules relating to the protection of network and information system security

Section 1: Security of the architecture

Rule 7. Configuration

The operator of critical services shall comply with the following rules when installing services and equipment on its critical information systems (CIS):

- the operator installs only those services and functionalities on its CIS that are essential to their running or security. It disables services and features that are not required, including those installed by default, and uninstalls them if possible. When un-installation is not possible, the operator shall mention this in the certification file of the relevant CIS, specifying the services and functionalities concerned and the risk reduction measures implemented;

- the operator only connects peripheral materials and removable media to its CIS equipment which it manages and which are critical for the running or security of its CIS;

- removable writable media connected to CIS are used exclusively for the running, including maintenance and administration, or security of CIS;

- the operator shall, before using any removable media, analyse their content, in particular for malicious code. The operator shall establish, on the equipment connecting to these removable media, mechanisms to protect against the risks of executing malicious from these media.

Rule 8. Partitioning

The operator of critical services shall partition its critical information systems (CIS) to limit the propagation of computer attacks within its systems or subsystems. It complies with the following rules:

- each CIS is physically or logically partitioned from the operator's other information systems and from third-party information systems;

- when a CIS is itself made up of subsystems, these are physically or logically partitioned from one another. A subsystem can be set up to ensure a functionality or a homogeneous set of functionalities of a CIS or to isolate resources of a CIS with the same security need;

- only those interconnections strictly required for the smooth running and security of a CIS shall be established between the CIS and other systems or between the subsystems of the CIS.

In the specific case of an interconnection between the Internet and a CIS necessary for the provision of domain name hosting, top level zone hosting, domain name resolution or peering interconnection for the exchange of Internet traffic, the operator need not ensure physical or logical partitioning at the level of that interconnection but must deploy appropriate protection measures such as those recommended by the National Agency for information systems security. Also, where a critical service requires the CIS necessary for its provision to be accessible via a public network, the operator shall organise that CIS, in line with the principle of in-depth defence, into at least two subsystems as follows:

- a first subsystem corresponding to the part of the CIS directly accessible via this public network, to which the operator applies appropriate partitioning measures such as those recommended by the National Agency for information systems security;

- a second subsystem corresponding to the internal part of the CIS to which the operator applies this partitioning rule.

The operator shall describe in the certification file for each CIS the partitioning mechanisms that it puts in place.

Rule 9. Remote access

The operator of critical services shall protect access to its critical information systems (CIS) through third-party information systems.

In particular, when an essential service requires the CIS necessary for its provision to be accessible via a public network, the operator must protect this access by means of cryptographic mechanisms that comply with the rules recommended by the National Agency for information systems security. Also, where the operator or a service provider appointed by the operator accesses a CIS via an information system which is not under the control of the operator or service provider, the operator must apply, or ensure that its service provider applies, the following rules:

- access to the CIS is protected by encryption and authentication mechanisms that comply with the rules recommended by the National Agency for Information Systems Security;

- when the CIS is accessed from a site external to that of the operator, the authentication mechanism is strengthened by implementing two-factor authentication (authentication involving both a secret element and another element specific to the user), unless technical or operational reasons, specified in the CIS certification file, do not allow it;

- the equipment used to access the CIS is managed and configured by the operator or, as applicable, by the service provider. When the CIS is accessed from a site outside the operator's premises, the mass memories of this equipment are permanently protected by encryption and authentication mechanisms that comply with the rules recommended by the National Agency for Information Systems Security.

The operator shall describe the mechanisms for protecting access to the CIS that it is putting in place, in the approval file for each CIS.

Rule 10. Filtering

The operator of critical services shall put mechanisms in place for filtering the data flows circulating in its critical information systems (CIS) to block the circulation of flows that are unnecessary for the running of its systems and likely to facilitate computer attacks. It complies with the following rules:

- the operator defines the rules for filtering data flows (filtering on network addresses, protocols, port numbers, etc.) to limit the circulation of flows to those necessary for the running and security of its CIS;

- the incoming and outgoing flows of the CIS as well as the flows between subsystems of CIS are filtered at the level of their interconnections such as to only allow the circulation of those flows which are strictly necessary for the running and security of the CIS. Flows that breach the filtering rules are blocked by default;

- the operator shall establish and maintain a list of filtering rules indicating all the rules in force or abolished within the last year. This list specifies for each rule:

- the reason for and date of implementation, modification or abolition of the rule;

- the technical details of the implementation of the rule.

In the specific case of a CIS required for the provision of peering interconnection service for the exchange of Internet traffic, the operator shall only implement filtering mechanisms for data flows other

than those corresponding to Internet traffic itself. The operator shall describe the filtering mechanisms that it implements in the certification file for each CIS.

Section 2: Security of administration

Rule 11. Administration accounts

The critical services operator creates accounts (called "administration accounts") intended only for persons (called "administrators") responsible for carrying out administration operations (installation, configuration, management, maintenance, supervision, etc.) of its critical information systems (CIS) resources.
The operator shall define, in accordance with its network and information system security policy, the rules for managing and assigning administration accounts for its CIS, and shall comply with the following rules:

- the allocation of rights to administrators respects the principle of least privilege (only strictly necessary rights are granted). In particular, to limit the scope of individual rights, they are assigned to each administrator by restricting them as far as possible to the functional and technical scope for which this administrator is responsible;

- An administration account is used exclusively to connect to an administration information system (information system used for the administration of resources) or to an administered resource;

- Administration operations are performed exclusively from administration accounts, and conversely, administration accounts are used exclusively for administration operations;

- where the administration of a resource cannot technically be carried out from a specific administration account, the operator shall put measures in place to ensure the traceability and control of the administration operations carried out on that resource and measures to reduce the risk associated with the use of a non-specific administration account. It describes these measures in the certification file of the CIS concerned as well as the technical reasons that prevented the use of an administration account;

- the operator prepares and maintains the list of administration accounts of its CIS and manages them as privileged accounts.

Rule 12. Administration information systems

The operator of critical services shall apply the following rules to the information systems (referred to as "administration information systems") used to administer its critical information systems (CIS):

- the hardware and software resources of administration information systems shall be managed and configured by the operator or, as applicable, by the service provider it has appointed to carry out the administration operations;

- the hardware and software resources of administration information systems are used exclusively to perform administration operations. However, when justified on technical or organisational grounds, the administrator's physical workstation may be used to perform non-administrative operations. In this case, mechanisms to harden and partition workstation operating systems must be put in place to isolate the software environment used for these other operations from the software environment used for administration operations;

- a software environment used to carry out administrative operations must not be used for other purposes, such as accessing websites or mail servers online;

- a user may not log on to an administrative information system using a software environment that is used for anything other than administrative operations;

- data flows associated with operations other than administration operations must, when transiting on administration information systems, be partitioned by encryption and authentication mechanisms that comply with the rules recommended by the National Agency for information systems security;

- the administration information systems are connected to the CIS resources to be administered through a physical network link used exclusively for administration operations. These resources are administered through their physical administration interface. When technical reasons prevent a resource from being administered over a physical network link or its physical administration interface, the operator shall take risk reduction measures such as logical security measures. In this case, it describes these measures and their justifications in the certification file of the relevant CIS;

- when they are not circulating in the administration information system, administration flows are protected by encryption and authentication mechanisms that comply with the rules recommended by the National Agency for Information Systems Security. If the encryption and authentication of these flows is not possible for technical reasons, the operator shall take measures to protect the confidentiality and integrity of these flows and to strengthen the control and traceability of administration operations. In this case, it describes these measures and their justifications in the certification file of the relevant CIS;

- logs recording events generated by management information system resources do not contain any passwords or other secret authentication elements in clear text or in the form of cryptographic fingerprints.

Section 3: Management of identities and access

Rule 13. Identification

The operator of critical services shall create individual accounts for all users (including users with privileged or administrative accounts) and for automatic processes accessing the resources of its critical information systems (CIS).

Where technical or operational reasons do not permit individual accounts to be created for users or for automatic processes, the operator shall put measures in place to reduce the risk associated with the use of shared accounts and to ensure the traceability of the use of such accounts. In this case, the operator describes these measures in the approval file of the relevant CIS and the reasons justifying the use of shared accounts.

Furthermore, where a critical service requires the dissemination of information to the public, the operator is not required to create accounts for public access to that information.

The operator shall immediately deactivate accounts that are no longer required.

Rule 14. Authentication

The operator of critical services shall protect access to the resources of its critical information systems (CIS), whether by a user or by an automated process, by means of an authentication mechanism involving a secret element.

The operator shall define, in accordance with its network and information system security policy, the rules for managing the secret authentication elements implemented in its CIS.

Where the resource technically permits it, the secret authentication elements must be modifiable by the operator whenever necessary. In this case, the operator shall comply with the following rules:

- the operator must modify the secret authentication elements when they have been installed by the manufacturer or supplier of the resource, before commissioning. To this end, the operator shall check with the manufacturer or supplier that it has the resources and rights to carry out these operations;

- the secret authentication element of a shared account must be renewed regularly and whenever a user withdraws from the account;

- users who are not responsible for them cannot change the secret authentication elements. They cannot also access these elements in clear;

- when the secret authentication elements are passwords, users may not reuse them between privileged accounts or between a privileged account and a non-privileged account;

- when the secret authentication elements are passwords, they comply with best practices such as those recommended by the National Agency for Information Systems Security, in terms of complexity (length of the password and types of characters), considering the maximum level of complexity allowed by the resource concerned, and in terms of renewal.

Where the resource does not technically permit the secret authentication element to be modified, the operator shall establish appropriate access checks to the resource concerned as well as measures to trace access and reduce the risk associated with the use of a fixed secret authentication element. The operator shall describe these measures and the technical reasons that prevented the modification of the secret authentication element in the approval file of the CIS concerned.

Furthermore, where a critical service requires the dissemination of information to the public, the operator is not required to put authentication mechanisms in place for public access to that information.

Rule 15. Access rights

The operator of critical services shall define, in accordance with its network and information systems security policy, the rules for managing and allocating access rights to its critical information systems (CIS) resources, and shall comply with the following rules:

- the operator only grants resource access rights to a user or to an automatic process if this access is strictly necessary for the performance of the user's duties or for the functioning of the automatic process;

- the operator defines the access to the different features of each resource and assigns rights only to those users and automatic processes that strictly need them;

- access rights are reviewed by the operator periodically, at least annually. This review focuses on the links between accounts, their associated access rights and the resources or features that are subject to them;

- the operator draws up and maintains a list of privileged accounts. Any change to a privileged account (addition, deletion, suspension or modification of the associated rights) is subject to a formal check by the operator in order to verify that the access rights to the resources and features are assigned according to the principle of least privilege (only strictly necessary rights are granted) and in a manner consistent with the usage needs of the account.

Section 4: Keeping secure

Rule 16. Procedure for keeping secure

The operator of critical services shall develop, maintain and implement a procedure for maintaining the security of its critical information systems (CIS) hardware and software resources in accordance with its network and information systems security policy.

This procedure defines the conditions for maintaining the level of security of CIS resources according to the evolution of vulnerabilities and threats, and sets out the policy for installing any new version and security patch for a resource and the checks to be carried out before installation. It provides that:

- the operator must keep itself informed of vulnerabilities and corrective patches likely to concern the hardware and software resources of its CIS, which are disseminated by the suppliers or manufacturers of these resources or by cyber security prevention and alert centres such as the CERT-FR (governmental centre for monitoring, alert and response to computer attacks);

- except in the case of justified technical or operational difficulties, the operator shall install and maintain all hardware and software resources of its CIS in versions which are supported by their suppliers or manufacturers and including security updates;

- before installing any new version, the operator must ensure the origin of this version and its integrity, and analyse its impact on the relevant CIS concerned from a technical and operational point of view;
- as soon as it becomes aware of a corrective safety measure concerning one of its resources, and except in the case of justified technical or operational difficulties, the operator must schedule its installation after carrying out the checks mentioned in the previous paragraph, within the time limits laid down in the procedure for maintaining security;

- where justified by technical or operational reasons, the operator may decide, when it comes to certain resources of its CIS, not to install a version supported by the supplier or manufacturer of the resource concerned or not to install a security fix. In this case, the operator must implement the technical or organisational measures provided for by the security maintenance procedure to reduce risks linked to the use of an obsolete version or one with known vulnerabilities. The operator shall describe these risk reduction measures and the technical or operational reasons that prevented the installation of a supported version or a security fix in the approval file of the relevant CIS.

Section 5: Physical and environmental security

Rule 17. Physical and environmental security

The operator of critical services shall define and implement, in accordance with its network and information systems security policy, the physical and environmental security procedures and measures applicable to its critical information systems (CIS). These procedures and measures include checks on internal and external personnel, the control of physical access to the CIS and, as applicable, the protection of the CIS against environmental risks such as natural disasters.

Chapter III: Rules relating to the defence of networks and information systems

Section 1: Detection of security incidents

Rule 18. Detection

The operator of critical services shall develop, maintain and implement, in accordance with its network and information systems security policy, a procedure for detecting security incidents affecting its critical information systems (CIS). This procedure sets out organisational and technical measures to detect security incidents affecting CIS. Oganisational measures include operating procedures for the detection devices and describe the sequence for processing security events identified by these devices. Technical measures specify the nature and positioning of the detection devices.
The operator deploys detection devices capable of identifying events characteristic of a security incident, particularly an ongoing or future attack, and of enabling the search for traces of previous incidents. To this end, these devices:

- collect relevant data on the operation of each CIS (in particular "network" or "system" data) from sensors positioned such as to identify the security events linked to all the data flows exchanged between the CIS and the operator's third-party information systems;

- Analyse sensor data by looking for known technical attack markers, to identify and characterise security events;

- archive the metadata of identified events to allow an a posteriori search for technical markers of attacks or compromises over a period of at least six months.

In the specific case of a CIS required for the provision of peering interconnection service for the exchange of Internet traffic, the operator shall only implement detection devices for data flows other than those corresponding to Internet traffic itself.

The operator or the service provider approved for this purpose operates the detection devices based on the requirements of the reference framework for the detection of security incidents adopted pursuant to Article 10 of Decree No. 2015-350 of 27 March 2015 as amended relating to the qualification of security products and trusted service providers for information system security purposes. The operator shall ensure that the installation and operation of detection devices does not affect the security and functioning of its CIS.

Rule 19. Logging

The operator of critical services shall implement a logging system on each critical information system (CIS) which records events relating to user authentication, account and access rights management, access to resources, changes to the CIS security rules and the operation of the CIS. The logging system helps detect security incidents by collecting log data.

The logging system shall cover the following equipment when it generates the events mentioned in the first subparagraph:

- application servers supporting essential services;

- system infrastructure servers;

- network infrastructure servers;

- security equipment;

- engineering and maintenance positions in industrial systems;

- network equipment;

- administrative positions.

Events recorded by the logging system are time-stamped using synchronised time sources. They are centralised and archived for a period of at least six months for each CIS. The event archiving format enables automated searches of these events.

Rule 20. Correlation and analysis of logs

The operator of critical services implements a log correlation and analysis system that exploits the events recorded by the logging system installed on each critical information system (CIS) to detect events that may affect the security of the CIS. The log correlation and analysis system helps detect security incidents by analysing log data. The log correlation and analysis system is installed and run on an information system set up exclusively for the purpose of detecting events that may affect the security of information systems.

The operator or the service provider approved for this purpose installs and operates this log correlation and analysis system based on the requirements of the reference framework for the detection of security incidents adopted pursuant to Article 10 of Decree No. 2015-350 of 27 March 2015 as amended relating to the qualification of security products and trusted service providers for information system security purposes.

Section 2: Management of security incidents

Rule 21. Response to incidents

The operator of critical services shall develop, maintain and implement, in accordance with its network and information systems security policy, a procedure for handling security incidents affecting its critical information systems (CIS). The operator or the service provider approved for this purpose processes incidents based on the requirements of the reference framework for the response to security incidents adopted pursuant to Article 10 of Decree No. 2015-350 of 27 March 2015 as amended relating to the qualification of security products and trusted service providers for information system security purposes. A specific information system must be put in place to process incidents, in particular to store technical records relating to the analysis of incidents. This system is compartmentalised with respect to the CIS involved in the incident.

The operator shall keep technical records relating to the analysis of incidents for a period of at least six months. It shall make these technical records available to the National Agency for the Security of Information Systems.

Rule 22. Processing of alerts

The operator of critical services shall set up a service enabling it to take note, as soon as possible, of information conveyed by the National Agency for information system security relating to incidents, vulnerabilities and threats. It shall deploy a procedure for processing the information thus received and, as applicable, take the necessary security measures to protect its critical information systems (CIS). The operator shall provide the National Agency for information systems security with the updated contact details (name of the department, telephone number and e-mail address) of the service provided for in the previous paragraph.

Chapter IV: Business resilience rules

Rule 23. Crisis management

The operator of critical services shall develop, keep up to date and implement, in accordance with its network and information systems security policy, a crisis management procedure in the event of security incidents having a major impact on the operator's critical services.

This procedure describes the crisis management organisation set up by the operator and provides for the application of the following technical measures to critical information systems (CIS):
- configure CIS in such a way as to avoid or limit the effects of attacks.

This configuration may include:

- prohibiting the use of removable storage media or the connection of mobile equipment to CIS;

- installing a security fix on a particular CIS;

- restricting routing;

- setting up filtering rules on networks or particular configurations on hardware. This measure may include:
- performing access restrictions in the form of user whitelists and blacklists;

- blocking file exchanges of a particular type;

- isolating the operator's websites, applications or computer equipment from any network;

- isolating the operator's CIS from the Internet. This measure requires the physical or logical disconnection of the network interfaces from the relevant CIS.

The procedure sets out the conditions under which these measures may be applied, taking into account the technical and organisational constraints of implementation.

Appendix II

Time limits for the application of security rules

SECURITY RULES	APPLICATION DEADLINES (from the date of designation of the operator as a critical service operator)
Rule 1. Risk analysis	**Deadline for security approval (Rule 3 deadline)**
Rule 2. Security policy	**1 year**
Rule 3. Security certification	**3 years for a critical information system (CIS) commissioned service prior to the date of designation of the operator of critical services.** **2 years for a CIS commissioned within 2 years of the date of designation of the operator of critical services.** **Before it is commissioned more than 2 years after the date of designation of the operator of critical services.**
Rule 4. Indicators	**2 years**
Rule 5. Security audits	**Deadline for security approval (Rule 3 deadline)**
Rule 6. Mapping	**1 year**

Rule 7. Configuration	**1 year**
Rule 8. Partitioning	**2 years**
Rule 9. Remote access	**2 years**
Rule 10. Filtering	**2 years**
Rule 11. Administration accounts	**2 years**
Rule 12. Administration information systems	**2 years**
Rule 13. Identification	**1 year**
Rule 14. Authentication	**1 year**
Rule 15. Access rights	**1 year**
Rule 16. Procedure for keeping secure	**1 year**
Rule 17. Physical and environmental security	**1 year**
Rule 18. Detection	**2 years**
Rule 19. Logging	**1 year**

Rule 20. Correlation and analysis of logs	**2 years**
Rule 21. Response to incidents	**1 year**
Rule 22. Processing of alerts	**3 months**
Rule 23. Crisis management	**1 year**

Done on 14 September 2018.