Official Journal
of the European Union

EN
L series

2024/2690

18.10.2024

COMMISSION IMPLEMENTING REGULATION (EU) 2024/2690

of 17 October 2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) ([1]), and in particular Articles 21(5), first subparagraph and 23(11), second subparagraph thereof,

Whereas:

(1) With regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers as covered by Article 3 of Directive (EU) 2022/2555 (the relevant entities), this Regulation aims to lay down the technical and the methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 and to further specify the cases in which an incident should be considered to be significant as referred to in Article 23(3) of Directive (EU) 2022/2555.

(2) Taking account of the cross-border nature of their activities and in order to ensure a coherent framework for trust service providers, this Regulation should, with respect to trust service providers, further specify the cases in which an incident shall be considered to be significant, in addition to laying down the technical and the methodological requirements of the cybersecurity risk-management measures.

(3) Following Article 21(5), third subparagraph of Directive (EU) 2022/2555, the technical and methodological requirements of the cybersecurity risk-management measures set out in the Annex to this Regulation are based on European and international standards, such as ISO/IEC 27001, ISO/IEC 27002 and ETSI EN 319401, and technical specifications, such as CEN/TS 18026:2024, relevant to the security of network and information systems.

(4) As regards the implementation and application of the technical and the methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation, in line with the principle of proportionality, due account should be taken of the divergent risk exposure of relevant entities, such as the criticality of the relevant entity, the risks to which it is exposed, the relevant entity's size and structure as well as the likelihood of occurrence of incidents and their severity, including their societal and economic impact, when complying with the technical and methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation.

([1]) OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) In line with the principle of proportionality, where relevant entities cannot implement some of the technical and the methodological requirements of the cybersecurity risk-management measures due to their size, those entities should be able to take other compensating measures that are suitable to achieve the purpose of those requirements. For example, when defining roles, responsibilities and authorities for network and information system security within the relevant entity, micro-sized entities might find it difficult to segregate conflicting duties and conflicting areas of responsibility. Such entities should be able to consider compensating measures such as targeted oversight by the entity's management or increased monitoring and logging.

(6) Certain technical and methodological requirements set out in the Annex to this Regulation should be applied by the relevant entities where appropriate, where applicable, or to the extent feasible. Where a relevant entity considers it not appropriate, not applicable or not feasible for the relevant entity to apply certain technical and methodological requirements as provided for in the Annex to this Regulation, the relevant entity should in a comprehensible manner document its reasoning to that effect. National competent authorities may, when exercising supervision, take into account the appropriate time required for the relevant entities to implement the technical and the methodological requirements of the cybersecurity risk-management measures.

(7) ENISA or national competent authorities under Directive (EU) 2022/2555 can provide guidance to support relevant entities in the identification, analysis, and assessment of risks for the purpose of implementing the technical and the methodological requirements concerning the establishment and maintenance of an appropriate risk management framework. Such guidance can include, in particular, national and sectoral risk assessments as well as risk assessments specific for a certain type of entity. The guidance may also include tools or templates for the development of risk management framework at the level of the relevant entities. Frameworks, guidance or other mechanisms provided by Member States' national law, as well as relevant European and international standards, can also support relevant entities in demonstrating compliance with this Regulation. Moreover, ENISA or national competent authorities under Directive (EU) 2022/2555 can support relevant entities in identifying and implementing appropriate solutions to treat risks identified in such risk assessments. Such guidance should be without prejudice to the relevant entities' obligation to identify and document the risks posed to the security of network and information systems, and to the relevant entities' obligation to implement the technical and the methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation according to their needs and resources.

(8) Network security measures in relation to: (i) the transition towards latest generation network layer communication protocols, (ii) the deployment of internationally agreed and interoperable modern email communications standards, and (iii) the application of best practices for DNS security, and for internet routing security and routing hygiene entail specific challenges regarding the identification of best available standards and deployment techniques. To achieve as soon as possible a high common level of cybersecurity across networks, the Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA) and in collaboration with competent authorities, industry – including telecommunication industry – and other stakeholders, should support the development of a multistakeholder forum tasked to identify these best available standards and deployment techniques. Such multi-stakeholder guidance should be without prejudice to the relevant entities' obligation to implement the technical and the methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation.

(9) Pursuant to Article 21(2), point (a), of Directive (EU) 2022/2555, essential and important entities should have, besides policies on risk analysis, policies on information system security. For that purpose, the relevant entities should establish a policy on the security of network and information systems as well as topic-specific policies, such as policies on access control, which should be coherent with the policy on the security of network and information systems. The policy on the security of network and information systems should be the highest-level document setting out the relevant entities' overall approach to their security of network and information systems and should be approved by the management bodies of the relevant entities. The topic-specific policies should be approved by an appropriate level of management. The policy should lay down indicators and measures to monitor its implementation and the current status of relevant entities' maturity level of network and information security, in particular to facilitate the oversight of the implementation of the cybersecurity risk-management measures through the management bodies.

(10) For the purposes of the technical and the methodological requirements laid down in the Annex to this Regulation, the term 'user' should encompass all legal and natural persons which have access to the entity's network and information systems.

(11) To identify and address the risks posed to the security of network and information systems, the relevant entities should establish and maintain an appropriate risk management framework. As a part of the risk management framework, the relevant entities should establish, implement and monitor a risk treatment plan. The relevant entities may use the risk treatment plan to identify and prioritise risk treatment options and measures. Options for risk treatment include, in particular, avoiding, reducing or, in exceptional cases, accepting the risk. The choice of risk treatment options should take into account the results of the risk assessment carried out by the relevant entity, and be in accordance with the relevant entity's policy on the security of network and information systems. To give effect to the chosen risk treatment options, the relevant entities should take the appropriate risk treatment measures.

(12) To detect events, near misses and incidents, the relevant entities should monitor their network and information systems and should take actions to evaluate events, near misses and incidents. Those measures should be capable of allowing the detection of network-based attacks based on anomalous inbound and outbound traffic patterns and denial of service attacks in a timely manner.

(13) When the relevant entities conduct a business impact analysis, they are encouraged to carry out a comprehensive analysis establishing, as appropriate, maximum tolerable downtime, recovery time objectives, recovery point objectives and service delivery objectives.

(14) In order to mitigate risks stemming from a relevant entity's supply chain and its relationship with its suppliers, the relevant entities should establish a supply chain security policy which governs their relations with their direct suppliers and service providers. These entities should specify in the contracts with their direct suppliers or service providers adequate security clauses, for example by requiring, where appropriate, cybersecurity risk-management measures according to Article 21(2) of Directive (EU) 2022/2555 or other similar legal requirements.

(15) The relevant entities should regularly carry out security tests based on a dedicated policy and procedures to verify whether the cybersecurity risk-management measures are implemented and function properly. Security tests may be performed on specific network and information systems or on the relevant entity as a whole and may include automated or manual tests, penetration tests, vulnerability scanning, static and dynamic application security tests, configuration tests or security audits. The relevant entities may conduct security tests on their network and information systems at set-up, after infrastructure or application upgrades or modifications that they deem significant, or after maintenance. The findings of the security tests should inform the relevant entities' policies and procedures to assess the effectiveness of the cybersecurity risk-management measures, as well as independent reviews of their network and information security policies.

(16) In order to avoid significant disruption and harm caused by the exploitation of unpatched vulnerabilities in network and information systems, the relevant entities should set out and apply appropriate security patch management procedures which are aligned with the relevant entities' change management, vulnerability management, risk management and other relevant procedures. Relevant entities should take measures proportionate to their resources to ensure that security patches do not introduce additional vulnerabilities or instabilities. In case of planned inaccessibility to the service caused by the application of security patches, the relevant entities are encouraged to duly inform customers in advance.

(17) The relevant entities should manage the risks stemming from the acquisition of ICT products or ICT services from suppliers or service providers and should obtain assurance that the ICT products or ICT services to be acquired achieve certain cybersecurity protection levels, for example by European cybersecurity certificates and EU statements of conformity for ICT products or ICT services issued under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council ([2]). Where the relevant entities set out security requirements to apply to the ICT products to be acquired, they should take into account the essential cybersecurity requirements set out in a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements.

(18) In order to protect against cyber threats and support the prevention and containment of data breaches, the relevant entities should implement network security solutions. Typical solutions for network security include the use of firewalls to protect the relevant entities' internal networks, the limitation of connections and access to services where connections and access are absolutely needed, and the use of virtual private networks for remote access and allowing connections of service providers only after an authorisation request and for a set time period such as the duration of a maintenance operation.

(19) In order to protect the networks of the relevant entities and their information systems against malicious and unauthorised software, those entities should implement controls that prevent or detect the use of unauthorised software and should, where appropriate, use detection and response software. The relevant entities should also consider implementing measures to minimize the attack surface, reduce vulnerabilities that can be exploited by attackers, control the execution of applications on endpoints, and deploy email and web application filters to reduce exposure to malicious content.

(20) Pursuant to Article 21(2), point (g), of Directive (EU) 2022/2555, Member States are to ensure that essential and important entities apply basic cyber hygiene practices and cybersecurity training. Basic cyber hygiene practices can include zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Cyber hygiene practices are a part of different technical and methodological requirements of the cybersecurity risk management measures set out in the Annex to this Regulation. With regard to basic cyber hygiene practices for users, the relevant entities should consider practices such as clear desk and screen policy, use of multi-factor and other authentication means, safe email use and web browsing, protection from phishing and social engineering, secure remote working practices.

(21) In order to prevent unauthorised access to the relevant entities' assets, the relevant entities should establish and implement a topic-specific policy addressing access by persons and by network and information systems, such as applications.

(22) In order to avoid that employees can misuse, for instance, access rights within the relevant entity to harm and cause damage, relevant entities should consider adequate employee security management measures and raise awareness among personnel about such risks. The relevant entities should establish, communicate and maintain a disciplinary process for handling violations of the relevant entities' network and information system security policies, which may be embedded in other disciplinary processes established by the relevant entities. Verification of the background of the employees and where applicable the direct suppliers and service providers of the relevant entities should contribute to the goal of human resources security in the relevant entities, and may include measures such as checks of the person's criminal record or past professional duties, as appropriate for the person's duties in the relevant entity and in line with the relevant entity's policy on the security of network and information systems.

([2]) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) Multi-factor authentication can enhance the entities' cybersecurity and should be considered by the entities in particular when users access network and information systems from remote locations, or when they access sensitive information or privileged accounts and system administration accounts. Multi-factor authentication can be combined with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.

(24) The relevant entities should manage and protect the assets which are of value to them through a sound asset management which should also serve as the basis for the risk analysis and business continuity management. The relevant entities should manage both tangible and intangible assets and should create an asset inventory, associate the assets with a defined classification level, handle and track the assets and take steps to protect the assets throughout their lifecycle.

(25) Asset management should involve classifying assets by their type, sensitivity, risk level, and security requirements and applying appropriate measures and controls to ensure their availability, integrity, confidentiality, and authenticity. By classifying assets by risk level, the relevant entities should be able to apply appropriate security measures and controls to protect assets such as encryption, access control including perimeter and physical and logical access control, backups, logging and monitoring, retention and disposal. When conducting a business impact analysis, the relevant entities may determine the classification level based on the consequences of disruption of assets for the entities. All employees of the entities handling assets should be familiar with the asset handling policies and instructions.

(26) The granularity of the asset inventory should be appropriate for the needs of the relevant entities. A comprehensive asset inventory could include, for each asset, at least a unique identifier, the owner of the asset, a description of the asset, the location of the asset, the type of asset, the type and classification of information processed in the asset, the date of last update or patch of the asset, the classification of the asset under the risk assessment, and the end of life of the asset. When identifying the owner of an asset, the relevant entities should also identify the person responsible for protecting said asset.

(27) The allocation and organisation of cybersecurity roles, responsibilities and authorities should establish a consistent structure for the governance and implementation of cybersecurity within the relevant entities, and should ensure effective communication in case of incidents. When defining and assigning responsibilities for certain roles, the relevant entities should consider roles such as chief information security officer, information security officer, incident handling officer, auditor, or comparable equivalents. Relevant entities may assign roles and responsibilities to external parties, such as ICT third-party service providers.

(28) In accordance with Article 21(2) of Directive (EU) 2022/2555, the cybersecurity risk-management measures are to be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity's information and information processing facilities, which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The technical and the methodological requirements of the cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena. Further examples of physical and environmental threats can include earthquakes, explosions, sabotage, insider threat, civil unrest, toxic waste, and environmental emissions. Prevention of loss, damage or compromise of network and information systems or interruption to their operations due to the failure and disruption of supporting utilities should contribute to the goal of business continuity in the relevant entities. Moreover, protection against physical and environmental threats should contribute to security of network and information systems maintenance in the relevant entities.

(29) Relevant entities should design and implement protection measures against physical and environmental threats and determine minimum and maximum control thresholds for physical and environmental threats and monitor environmental parameters. For example, they should consider installing systems to detect at an early stage the flooding of areas where network and information systems are located. Regarding fire hazard, the relevant entities should consider the establishment of a separate fire compartment for the data centre, the use of fire-resistant materials, sensors for monitoring temperature and humidity, the connection of the building to a fire alarm system with an automated notification to the local fire department, and early fire detection and extinguishing systems. The relevant entities should also carry out regular fire drills and fire inspections. Furthermore, to ensure power supply, the relevant entities should consider overvoltage protection and corresponding emergency power supply, in accordance with relevant standards. Moreover, as overheating poses a risk to the availability of network and information systems, relevant entities, in particular data centre service providers, could consider adequate, continuous and redundant air conditioning systems.

(30) This Regulation is to further specify the cases in which an incident should be considered to be significant for the purpose of Article 23(3) of Directive (EU) 2022/2555. The criteria should be such that relevant entities are able to assess whether an incident is significant, in order to notify the incident in accordance with Directive (EU) 2022/2555. Furthermore, the criteria set out in this Regulation should be considered exhaustive, without prejudice to Article 5 of Directive (EU) 2022/2555. This regulation specifies the cases in which an incident should be considered to be significant by setting out horizontal as well as entity-type specific cases.

(31) Pursuant to Article 23(4) of Directive (EU) 2022/2555, relevant entities should be required to notify significant incidents within the deadlines set by that provision. Those notification deadlines are running from the moment the entity becomes aware of such significant incidents. The relevant entity is therefore required to report incidents that, based on its initial assessment, could cause severe operational disruption of the services or financial loss for that entity or affect other natural or legal persons by causing considerable material or non-material damage. Therefore, when a relevant entity has detected a suspicious event, or after a potential incident has been brought to its attention by a third party, such as an individual, a customer, an entity, an authority, a media organisation, or another source, the relevant entity should assess in a timely manner the suspicious event to determine whether it constitutes an incident and, if so, determine its nature and severity. The relevant entity is therefore to be regarded as having become 'aware' of the significant incident when, after such initial assessment, that entity has a reasonable degree of certainty that a significant incident has occurred.

(32) With a view to establishing whether an incident is significant, where relevant, relevant entities should count the number of users impacted by the incident, taking into consideration business and end customers with whom the relevant entities have a contractual relationship as well as natural and legal persons that are associated with business customers. Where a relevant entity is unable to calculate the number of impacted users, the relevant entity's estimate of the possible maximum number of affected users should be considered for the purpose of calculating the total number of users affected by the incident. The significance of an incident involving a trust service should not only be determined by the number of users but also by the number of relying parties as these can be equally affected by a significant incident involving a trust service in regard to operational disruption and material or non-material damage. Therefore, trust service providers should, where applicable, also take into account the number of relying parties when establishing whether an incident is significant. For that purpose, relying parties should be understood as natural or legal persons that rely upon a trust service.

(33) Maintenance operations resulting in the limited availability or unavailability of the services should not be considered as significant incidents if the limited availability or unavailability of the service occurs according to a scheduled maintenance operation. Moreover, where a service is unavailable due to scheduled interruptions such as interruptions or non-availability based on pre-determined contractual agreement should not be considered as significant incident.

(34) The duration of an incident which impacts availability of a service should be measured from the disruption of the proper provision of such service until the time of recovery. Where a relevant entity is unable to determine the moment when the disruption began, the duration of the incident should be measured from the moment the incident was detected, or from the moment when the incident was recorded in network or system logs or other data sources, whichever is earlier.

(35) Complete unavailability of a service should be measured from the moment the service is fully unavailable to users, to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident. Where a relevant entity is unable to determine when the complete unavailability of a service began, the unavailability should be measured from the moment it was detected by that entity.

(36) For the purpose of determining the direct financial losses resulting from an incident, relevant entities should take into account all the financial losses which they have incurred as a result of the incident, such as costs for replacement or relocation of software, hardware or infrastructure, staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills, fees due to non-compliance with contractual obligations, costs for redress and compensation to customers, losses due to forgone revenues, costs associated with internal and external communication, advisory costs, including costs associated with legal counselling, forensic services and remediation services, and other costs associated to the incident. However, administrative fines, as well as costs that are necessary for the day-to-day operation of the business, should not be considered as financial losses resulting from an incident, including costs for general maintenance of infrastructure, equipment, hardware and software, keeping skills of staff up to date, internal or external costs to enhance the business after the incident, including upgrades, improvements and risk assessment initiatives, and insurance premiums. The relevant entities should calculate the amounts of financial losses based on available data and, where the actual amounts of financial losses cannot be determined, the entities should estimate those amounts.

(37) Relevant entities should also be obliged to report incidents that have caused or are capable of causing the death of natural persons or considerable damage to natural persons' health as such incidents are particularly serious cases of causing considerable material or non-material damage. For instance, an incident affecting a relevant entity could cause unavailability of healthcare or emergency services, or the loss of confidentiality or integrity of data with an effect on the health of natural persons. For the purpose of determining whether an incident has caused or is capable of causing considerable damage to a natural person's health, relevant entities should take into account whether the incident caused or is capable of causing severe injuries and ill-health. For that purpose, the relevant entities should not be required to collect additional information to which they do not have access.

(38) Limited availability should be considered to occur in particular when a service provided by a relevant entity is considerably slower than average response time, or where not all functionalities of a service are available. Where possible, objective criteria based on the average response times of services provided by the relevant entities should be used to assess delays in response time. A functionality of a service may be, for instance, a chat functionality or an image search functionality.

(39) Successful, suspectedly malicious and unauthorised access to a relevant entity's network and information systems should be regarded as a significant incident, where such access is capable of causing severe operational disruption. For instance, where a cyber threat actor pre-positions itself in a relevant entity's network and information systems with a view to causing disruption of services in the future, the incident should be considered to be significant.

(40) Recurring incidents that are linked through the same apparent root cause, which individually do not meet the criteria of a significant incident, should collectively be considered to be a significant incident, provided that they collectively meet the criterion for financial loss, and that they have occurred at least twice within six months. Such recurring incidents can indicate significant deficiencies and weaknesses in the relevant entity's cybersecurity risk management procedures and their level of cybersecurity maturity. Moreover, such recurring incidents are capable of causing significant financial loss for the relevant entity.

(41) The Commission has exchanged advice and cooperated with the Cooperation Group and ENISA on the draft implementing act, in accordance with Articles 21(5) and 23(11) of Directive (EU) 2022/2555.

(42) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([3]), and delivered its opinion on 1 September 2024.

(43) The measures provided for in this Regulation are in accordance with the opinion of the committee established in accordance with Article 39 of Directive (EU) 2022/2555,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (the relevant entities) lays down the technical and the methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 and further specifies the cases in which an incident shall be considered to be significant as referred to in Article 23(3) of Directive (EU) 2022/2555.

Article 2

Technical and methodological requirements

1. For the relevant entities the technical and methodological requirements of cybersecurity risk-management measures referred to in Article 21(2), points (a) to (j), of Directive (EU) 2022/2555 are set out in the Annex to this Regulation.

2. The relevant entities shall ensure a level of security of network and information systems appropriate to the risks posed when implementing and applying the technical and methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation. For that purpose, they shall take due account of the degree of their exposure to risks, their size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact, when complying with the technical and methodological requirements of cybersecurity risk-management measures set out in the Annex to this Regulation.

([3]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Where the Annex to this Regulation provides that a technical or methodological requirement of a cybersecurity risk-management measure shall be applied 'where appropriate', 'where applicable' or 'to the extent feasible', and where a relevant entity considers it not appropriate, not applicable or not feasible for the relevant entity to apply certain such technical and methodological requirements, the relevant entity shall in a comprehensible manner document its reasoning to that effect.

Article 3

Significant incidents

1. An incident shall be considered to be significant for the purposes of Article 23(3) of Directive (EU) 2022/2555 with regard to the relevant entities where one or more of the following criteria are fulfilled:

(a) the incident has caused or is capable of causing direct financial loss for the relevant entity that exceeds EUR 500 000 or 5 % of the relevant entity's total annual turnover in the preceding financial year, whichever is lower;

(b) the incident has caused or is capable of causing the exfiltration of trade secrets as set out in Article 2 point (1), of Directive (EU) 2016/943 of the relevant entity;

(c) the incident has caused or is capable of causing the death of a natural person;

(d) the incident has caused or is capable of causing considerable damage to a natural person's health;

(e) a successful, suspectedly malicious and unauthorised access to network and information systems occurred, which is capable of causing severe operational disruption;

(f) the incident meets the criteria set out in Article 4;

(g) the incident meets one or more of the criteria set out in Articles 5 to 14.

2. Scheduled interruptions of service and planned consequences of scheduled maintenance operations carried out by or on behalf of the relevant entities shall not be considered to be significant incidents.

3. When calculating the number of users impacted by an incident for the purpose of Articles 7 and 9 to 14, the relevant entities shall consider all of the following:

(a) the number of customers that have a contract with the relevant entity which grants them access to the relevant entity's network and information systems or services offered by, or accessible via, those network and information systems;

(b) the number of natural and legal persons associated with business customers that use the entities' network and information systems or services offered by, or accessible via, those network and information systems.

Article 4

Recurring incidents

Incidents that individually are not considered a significant incident within the meaning of Article 3, shall be considered collectively as one significant incident where they meet all of the following criteria:

(a) they have occurred at least twice within 6 months;

(b) they have the same apparent root cause;

(c) they collectively meet the criteria set out in Article 3(1)(a).

Article 5

Significant incidents with regard to DNS service providers

With regard to DNS service providers, an incident shall be considered significant under Article 3(1)(g), where it fulfils one or more of the following criteria:

(a) a recursive or authoritative domain name resolution service is completely unavailable for more than 30 minutes;

(b) for a period of more than one hour, the average response time of a recursive or authoritative domain name resolution service to DNS requests is more than 10 seconds;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of the authoritative domain name resolution service is compromised, except in cases where the data of fewer than 1 000 domain names managed by the DNS service provider, amounting to no more than 1 % of the domain names managed by the DNS service provider, are not correct because of misconfiguration.

Article 6

Significant incidents with regard to TLD name registries

With regard to TLD name registries, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) an authoritative domain name resolution service is completely unavailable;

(b) for a period of more than one hour, the average response time of an authoritative domain name resolution service to DNS requests is more than 10 seconds,

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the technical operation of the TLD is compromised.

Article 7

Significant incidents with regard to cloud computing service providers

With regard to cloud computing service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a cloud computing service provided is completely unavailable for more than 30 minutes;

(b) the availability of a cloud computing service of a provider is limited for more than 5 % of the cloud computing service's users in the Union, or for more than 1 million of the cloud computing service's users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a cloud computing service is compromised as a result of a suspectedly malicious action,

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a cloud computing service is compromised with an impact on more than 5 % of that cloud computing service's users in the Union, or on more than 1 million of that cloud computing service's users in the Union, whichever number is smaller.

Article 8

Significant incidents with regard to data centre service providers

With regard to data centre service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a data centre service of a data centre operated by the provider is completely unavailable;

(b) the availability of a data centre service of a data centre operated by the provider is limited for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a data centre service is compromised as a result of a suspectedly malicious action;

(d) physical access to a data centre operated by the provider is compromised.

Article 9

Significant incidents with regard to content delivery network providers

With regard to content delivery network providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a content delivery network is completely unavailable for more than 30 minutes;

(b) the availability of a content delivery network is limited for more than 5 % of the content delivery network's users in the Union, or for more than 1 million of the content delivery network's users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a content delivery network is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a content delivery network is compromised with an impact on more than 5 % of that content delivery network's users in the Union, or on more than 1 million of that content delivery network's users in the Union, whichever number is smaller.

Article 10

Significant incidents with regard to managed service providers and managed security service providers

With regard to managed service providers and managed security service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a managed service or managed security service is completely unavailable for more than 30 minutes;

(b) the availability of a managed service or managed security service is limited for more than 5 % of the service's users in the Union, or for more than 1 million of the service's users in the Union, whichever number is smaller, for a duration of more than one hour;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a managed service or managed security service is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a managed service or a managed security service, is compromised with an impact on more than 5 % of that managed service's or that managed security service's users in the Union, or on more than 1 million of the service users in the Union, whichever number is smaller.

Article 11

Significant incidents with regard to providers of online marketplaces

With regard to providers of online marketplaces, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) an online marketplace is completely unavailable for more than 5 % of an online marketplace's users in the Union, or for more than 1 million of an online marketplace's users in the Union, whichever number is smaller;

(b) more than 5 % of an online marketplace's users in the Union, or more than 1 million of an online marketplace's users in the Union, whichever number is smaller, are impacted by limited availability of that online marketplace;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online marketplace is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online marketplace is compromised with an impact on more than 5 % of that online marketplace's users in the Union, or on more than 1 million of that online marketplace's users in the Union, whichever number is smaller.

Article 12

Significant incidents with regard to providers of online search engines

With regard to providers of online search engines, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) an online search engine is completely unavailable for more than 5 % of that online search engine's users in the Union, or for more than 1 million of that online search engine's users in the Union, whichever number is smaller;

(b) more than 5 % of an online search engine's users in the Union, or more than 1 million of an online search engine's users in the Union, whichever number is smaller, are impacted by limited availability of that online search engine;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online search engine is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of an online search engine is compromised with an impact on more than 5 % of that online search engine's users in the Union, or on more than 1 million of that online search engine's users in the Union, whichever number is smaller.

Article 13

Significant incidents with regard to providers of social networking services platforms

With regard to providers of social networking services platforms, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a social networking service platform is completely unavailable for more than 5 % of that social networking service platform's users in the Union, or for more than 1 million of that social networking service platform's users in the Union, whichever number is smaller;

(b) more than 5 % of a social networking service platform's users in the Union, or more than 1 million of a social networking service platform's users in the Union, whichever number is smaller, are impacted by limited availability of that social networking service platform;

(c) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a social networking service platform is compromised as a result of a suspectedly malicious action;

(d) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a social networking service platform is compromised with an impact on more than 5 % of that social networking service platform's users in the Union, or on more than 1 million of that social networking service platform's users in the Union, whichever number is smaller.

Article 14

Significant incidents with regard to trust service providers

With regard to trust service providers, an incident shall be considered significant under Article 3(1)(g) where it fulfils one or more of the following criteria:

(a) a trust service is completely unavailable for more than 20 minutes;

(b) a trust service is unavailable to users, or relying parties, for more than one hour calculated on a calendar week basis;

(c) more than 1 % of the users or relying parties in the Union, or more than 200 000 users or relying parties in the Union, whichever number is smaller, are impacted by limited availability of a trust service;

(d) physical access to an area where network and information systems are located and to which access is restricted to trusted personnel of the trust service provider, or the protection of such physical access, is compromised;

(e) the integrity, confidentiality or authenticity of stored, transmitted or processed data related to the provision of a trust service is compromised with an impact on more than 0,1 % of users or relying parties, or more than 100 of users or relying parties, whichever number is smaller, of the trust service in the Union.

Article 15

Repeal

Commission Implementing Regulation (EU) 2018/151 ([4]) is repealed.

Article 16

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 17 October 2024.

For the Commission
Ursula VON DER LEYEN
The President

([4]) Commission 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 (OJ L 26, 31.1.2018, p. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

ANNEX

Technical and methodological requirements referred to in Article 2 of this Regulation

1. **Policy on the security of network and information systems (Article 21(2), point (a) of Directive (EU) 2022/2555)**

1.1. *Policy on the security of network and information systems*

1.1.1. For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the policy on the security of network and information systems shall:

(a) set out the relevant entities' approach to managing the security of their network and information systems;

(b) be appropriate to and complementary with the relevant entities' business strategy and objectives;

(c) set out network and information security objectives;

(d) include a commitment to continual improvement of the security of network and information systems;

(e) include a commitment to provide the appropriate resources needed for its implementation, including the necessary staff, financial resources, processes, tools and technologies;

(f) be communicated to and acknowledged by relevant employees and relevant interested external parties;

(g) lay down roles and responsibilities pursuant to point 1.2;

(h) list the documentation to be kept and the duration of retention of the documentation;

(i) list the topic-specific policies;

(j) lay down indicators and measures to monitor its implementation and the current status of relevant entities' maturity level of network and information security;

(k) indicate the date of the formal approval by the management bodies of the relevant entities (the 'management bodies').

1.1.2. The network and information system security policy shall be reviewed and, where appropriate, updated by management bodies at least annually and when significant incidents or significant changes to operations or risks occur. The result of the reviews shall be documented.

1.2. *Roles, responsibilities and authorities*

1.2.1. As part of their policy on the security of network and information systems referred to in point 1.1, the relevant entities shall lay down responsibilities and authorities for network and information system security and assign them to roles, allocate them according to the relevant entities' needs, and communicate them to the management bodies.

1.2.2. The relevant entities shall require all personnel and third parties to apply network and information system security in accordance with the established network and information security policy, topic-specific policies and procedures of the relevant entities.

1.2.3. At least one person shall report directly to the management bodies on matters of network and information system security.

1.2.4. Depending on the size of the relevant entities, network and information system security shall be covered by dedicated roles or duties carried out in addition to existing roles.

1.2.5. Conflicting duties and conflicting areas of responsibility shall be segregated, where applicable.

1.2.6. Roles, responsibilities and authorities shall be reviewed and, where appropriate, updated by management bodies at planned intervals and when significant incidents or significant changes to operations or risks occur.

2. **Risk management policy (Article 21(2), point (a) of Directive (EU) 2022/2555)**

2.1. *Risk management framework*

2.1.1. For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by management bodies or, where applicable, by persons who are accountable and have the authority to manage risks, provided that the relevant entities ensure adequate reporting to the management bodies.

2.1.2. For the purpose of point 2.1.1, the relevant entities shall establish procedures for identification, analysis, assessment and treatment of risks ('cybersecurity risk management process'). The cybersecurity risk management process shall be an integral part of the relevant entities' overall risk management process, where applicable. As part of the cybersecurity risk management process, the relevant entities shall:

(a) follow a risk management methodology;

(b) establish the risk tolerance level in accordance with the risk appetite of the relevant entities;

(c) establish and maintain relevant risk criteria;

(d) in line with an all-hazards approach, identify and document the risks posed to the security of network and information systems, in particular in relation to third parties and risks that could lead to disruptions in the availability, integrity, authenticity and confidentiality of the network and information systems, including the identification of single point of failures;

(e) analyse the risks posed to the security of network and information systems, including threat, likelihood, impact, and risk level, taking into account cyber threat intelligence and vulnerabilities;

(f) evaluate the identified risks based on the risk criteria;

(g) identify and prioritise appropriate risk treatment options and measures;

(h) continuously monitor the implementation of the risk treatment measures;

(i) identify who is responsible for implementing the risk treatment measures and when they should be implemented;

(j) document the chosen risk treatment measures in a risk treatment plan and the reasons justifying the acceptance of residual risks in a comprehensible manner.

2.1.3. When identifying and prioritising appropriate risk treatment options and measures, the relevant entities shall take into account the risk assessment results, the results of the procedure to assess the effectiveness of cybersecurity risk-management measures, the cost of implementation in relation to the expected benefit, the asset classification referred to in point 12.1, and the business impact analysis referred to in point 4.1.3.

2.1.4. The relevant entities shall review and, where appropriate, update the risk assessment results and the risk treatment plan at planned intervals and at least annually, and when significant changes to operations or risks or significant incidents occur.

2.2. *Compliance monitoring*

2.2.1. The relevant entities shall regularly review the compliance with their policies on network and information system security, topic-specific policies, rules, and standards. The management bodies shall be informed of the status of network and information security on the basis of the compliance reviews by means of regular reporting.

2.2.2. The relevant entities shall put in place an effective compliance reporting system which shall be appropriate to their structures, operating environments and threat landscapes. The compliance reporting system shall be capable to provide to the management bodies an informed view of the current state of the relevant entities' management of risks.

2.2.3. The relevant entities shall perform the compliance monitoring at planned intervals and when significant incidents or significant changes to operations or risks occur.

2.3. *Independent review of information and network security*

2.3.1. The relevant entities shall review independently their approach to managing network and information system security and its implementation including people, processes and technologies.

2.3.2. The relevant entities shall develop and maintain processes to conduct independent reviews which shall be carried out by individuals with appropriate audit competence. Where the independent review is conducted by staff members of the relevant entity, the persons conducting the reviews shall not be in the line of authority of the personnel of the area under review. If the size of the relevant entities does not allow such separation of line of authority, the relevant entities shall put in place alternative measures to guarantee the impartiality of the reviews.

2.3.3. The results of the independent reviews, including the results from the compliance monitoring pursuant to point 2.2 and the monitoring and measurement pursuant to point 7, shall be reported to the management bodies. Corrective actions shall be taken or residual risk accepted according to the relevant entities' risk acceptance criteria.

2.3.4. The independent reviews shall take place at planned intervals and when significant incidents or significant changes to operations or risks occur.

3. **Incident handling (Article 21(2), point (b), of Directive (EU) 2022/2555)**

3.1. *Incident handling policy*

3.1.1. For the purpose of Article 21(2), point (b) of Directive (EU) 2022/2555, the relevant entities shall establish and implement an incident handling policy laying down the roles, responsibilities, and procedures for detecting, analysing, containing or responding to, recovering from, documenting and reporting of incidents in a timely manner.

3.1.2. The policy referred to in point 3.1.1 shall be coherent with the business continuity and disaster recovery plan referred to in point 4.1. The policy shall include:

(a) a categorisation system for incidents that is consistent with the event assessment and classification carried out pursuant to point 3.4.1;

(b) effective communication plans including for escalation and reporting;

(c) assignment of roles to detect and appropriately respond to incidents to competent employees;

(d) documents to be used in the course of incident detection and response such as incident response manuals, escalation charts, contact lists and templates.

3.1.3. The roles, responsibilities and procedures laid down in the policy shall be tested and reviewed and, where appropriate, updated at planned intervals and after significant incidents or significant changes to operations or risks.

3.2. *Monitoring and logging*

3.2.1. The relevant entities shall lay down procedures and use tools to monitor and log activities on their network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.

3.2.2. To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to business capabilities. The relevant entities shall implement their monitoring activities in a way which minimises false positives and false negatives.

3.2.3. Based on the procedures referred to in point 3.2.1, the relevant entities shall maintain, document, and review logs. The relevant entities shall establish a list of assets to be subject to logging based on the results of the risk assessment carried out pursuant to point 2.1. Where appropriate, logs shall include:

(a) relevant outbound and inbound network traffic;

(b) creation, modification or deletion of users of the relevant entities' network and information systems and extension of the permissions;

(c) access to systems and applications;

(d) authentication-related events;

(e) all privileged access to systems and applications, and activities performed by administrative accounts;

(f) access or changes to critical configuration and backup files;

(g) event logs and logs from security tools, such as antivirus, intrusion detection systems or firewalls;

(h) use of system resources, as well as their performance;

(i) physical access to facilities;

(j) access to and use of their network equipment and devices;

(k) activation, stopping and pausing of the various logs;

(l) environmental events.

3.2.4. The logs shall be regularly reviewed for any unusual or unwanted trends. Where appropriate, the relevant entities shall lay down appropriate values for alarm thresholds. If the laid down values for alarm threshold are exceeded, an alarm shall be triggered, where appropriate, automatically. The relevant entities shall ensure that, in case of an alarm, a qualified and appropriate response is initiated in a timely manner.

3.2.5. The relevant entities shall maintain and back up logs for a predefined period and shall protect them from unauthorised access or changes.

3.2.6. To the extent feasible, the relevant entities shall ensure that all systems have synchronised time sources to be able to correlate logs between systems for event assessment. The relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant. The availability of the monitoring and logging systems shall be monitored independent of the systems they are monitoring.

3.2.7. The procedures as well as the list of assets that are being logged shall be reviewed and, where appropriate, updated at regular intervals and after significant incidents.

3.3. *Event reporting*

3.3.1. The relevant entities shall put in place a simple mechanism allowing their employees, suppliers, and customers to report suspicious events.

3.3.2. The relevant entities shall, where appropriate, communicate the event reporting mechanism to their suppliers and customers, and shall regularly train their employees how to use the mechanism.

3.4. *Event assessment and classification*

3.4.1. The relevant entities shall assess suspicious events to determine whether they constitute incidents and, if so, determine their nature and severity.

3.4.2. For the purpose of point 3.4.1, the relevant entities shall act in the following manner:

(a) carry out the assessment based on predefined criteria laid down in advance, and on a triage to determine prioritisation of incident containment and eradication;

(b) assess the existence of recurring incidents as referred to in Article 4 of this Regulation on a quarterly basis;

(c) review the appropriate logs for the purposes of event assessment and classification;

(d) put in place a process for log correlation and analysis, and

(e) reassess and reclassify events in case of new information becoming available or after analysis of previously available information.

3.5. *Incident response*

3.5.1. The relevant entities shall respond to incidents in accordance with documented procedures and in a timely manner.

3.5.2. The incident response procedures shall include the following stages:

(a) incident containment, to prevent the consequences of the incident from spreading;

(b) eradication, to prevent the incident from continuing or reappearing,

(c) recovery from the incident, where necessary.

3.5.3. The relevant entities shall establish communication plans and procedures:

(a) with the Computer Security Incident Response Teams (CSIRTs) or, where applicable, the competent authorities, related to incident notification;

(b) for communication among staff members of the relevant entity, and for communication with relevant stakeholders external to the relevant entity.

3.5.4. The relevant entities shall log incident response activities in accordance with the procedures referred to in point 3.2.1, and record evidence.

3.5.5. The relevant entities shall test at planned intervals their incident response procedures.

3.6. *Post-incident reviews*

3.6.1. Where appropriate, the relevant entities shall carry out post-incident reviews after recovery from incidents. The post-incident reviews shall identify, where possible, the root cause of the incident and result in documented lessons learned to reduce the occurrence and consequences of future incidents.

3.6.2. The relevant entities shall ensure that post-incident reviews contribute to improving their approach to network and information security, to risk treatment measures, and to incident handling, detection and response procedures.

3.6.3. The relevant entities shall review at planned intervals if incidents led to post-incident reviews.

4. **Business continuity and crisis management (Article 21(2), point (c), of Directive (EU) 2022/2555)**

4.1. *Business continuity and disaster recovery plan*

4.1.1. For the purpose of Article 21(2), point (c) of Directive (EU) 2022/2555, the relevant entities shall lay down and maintain a business continuity and disaster recovery plan to apply in the case of incidents.

4.1.2. The relevant entities' operations shall be restored according to the business continuity and disaster recovery plan. The plan shall be based on the results of the risk assessment carried out pursuant to point 2.1 and shall include, where appropriate, the following:

(a) purpose, scope and audience;

(b) roles and responsibilities;

(c) key contacts and (internal and external) communication channels;

(d) conditions for plan activation and deactivation;

(e) order of recovery for operations;

(f) recovery plans for specific operations, including recovery objectives;

(g) required resources, including backups and redundancies;

(h) restoring and resuming activities from temporary measures.

4.1.3. The relevant entities shall carry out a business impact analysis to assess the potential impact of severe disruptions to their business operations and shall, based on the results of the business impact analysis, establish continuity requirements for the network and information systems.

4.1.4. The business continuity plan and disaster recovery plan shall be tested, reviewed and, where appropriate, updated at planned intervals and following significant incidents or significant changes to operations or risks. The relevant entities shall ensure that the plans incorporate lessons learnt from such tests.

4.2. *Backup and redundancy management*

4.2.1. The relevant entities shall maintain backup copies of data and provide sufficient available resources, including facilities, network and information systems and staff, to ensure an appropriate level of redundancy.

4.2.2. Based on the results of the risk assessment carried out pursuant to point 2.1 and the business continuity plan, the relevant entities shall lay down backup plans which include the following:

(a) recovery times;

(b) assurance that backup copies are complete and accurate, including configuration data and data stored in cloud computing service environment;

(c) storing backup copies (online or offline) in a safe location or locations, which are not in the same network as the system, and are at sufficient distance to escape any damage from a disaster at the main site;

(d) appropriate physical and logical access controls to backup copies, in accordance with the asset classification level;

(e) restoring data from backup copies;

(f) retention periods based on business and regulatory requirements.

4.2.3. The relevant entities shall perform regular integrity checks on the backup copies.

4.2.4. Based on the results of the risk assessment carried out pursuant to point 2.1 and the business continuity plan, the relevant entities shall ensure sufficient availability of resources by at least partial redundancy of the following:

(a) network and information systems;

(b) assets, including facilities, equipment and supplies;

(c) personnel with the necessary responsibility, authority and competence;

(d) appropriate communication channels.

4.2.5. Where appropriate, the relevant entities shall ensure that monitoring and adjustment of resources, including facilities, systems and personnel, is duly informed by backup and redundancy requirements.

4.2.6. The relevant entities shall carry out regular testing of the recovery of backup copies and redundancies to ensure that, in recovery conditions, they can be relied upon and cover the copies, processes and knowledge to perform an effective recovery. The relevant entities shall document the results of the tests and, where needed, take corrective action.

4.3. *Crisis management*

4.3.1. The relevant entities shall put in place a process for crisis management.

4.3.2. The relevant entities shall ensure that the crisis management process addresses at least the following elements:

(a) roles and responsibilities for personnel and, where appropriate, suppliers and service providers, specifying the allocation of roles in crisis situations, including specific steps to follow;

(b) appropriate communication means between the relevant entities and relevant competent authorities;

(c) application of appropriate measures to ensure the maintenance of network and information system security in crisis situations.

For the purpose of point (b), the flow of information between the relevant entities and relevant competent authorities shall include both obligatory communications, such as incident reports and related timelines, and non-obligatory communications.

4.3.3. The relevant entities shall implement a process for managing and making use of information received from the CSIRTs or, where applicable, the competent authorities, concerning incidents, vulnerabilities, threats or possible mitigation measures.

4.3.4. The relevant entities shall test, review and, where appropriate, update the crisis management plan on a regular basis or following significant incidents or significant changes to operations or risks.

5. **Supply chain security (Article 21(2), point (d), of Directive (EU) 2022/2555)**

5.1. *Supply chain security policy*

5.1.1. For the purpose of Article 21(2), point (d) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.

5.1.2. As part of the supply chain security policy referred to in point 5.1.1, the relevant entities shall lay down criteria to select and contract suppliers and service providers. Those criteria shall include the following:

(a) the cybersecurity practices of the suppliers and service providers, including their secure development procedures;

(b) the ability of the suppliers and service providers to meet cybersecurity specifications set by the relevant entities;

(c) the overall quality and resilience of ICT products and ICT services and the cybersecurity risk-management measures embedded in them, including the risks and classification level of the ICT products and ICT services;

(d) the ability of the relevant entities to diversify sources of supply and limit vendor lock-in, where applicable.

5.1.3. When establishing their supply chain security policy, relevant entities shall take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555, where applicable.

5.1.4. Based on the supply chain security policy and taking into account the results of the risk assessment carried out in accordance with point 2.1 of this Annex, the relevant entities shall ensure that their contracts with the suppliers and service providers specify, where appropriate through service level agreements, the following, where appropriate:

(a) cybersecurity requirements for the suppliers or service providers, including requirements as regards the security in acquisition of ICT services or ICT products set out in point 6.1;

(b) requirements regarding awareness, skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees;

(c) requirements regarding the verification of the background of the suppliers' and service providers' employees;

(d) an obligation on suppliers and service providers to notify, without undue delay, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities;

(e) the right to audit or right to receive audit reports;

(f) an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of the relevant entities;

(g) requirements regarding subcontracting and, where the relevant entities allow subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point (a);

(h) obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks.

5.1.5. The relevant entities shall take into account the elements referred to in point 5.1.2 and 5.1.3 as part of the selection process of new suppliers and service providers, as well as part of the procurement process referred to in point 6.1.

5.1.6. The relevant entities shall review the supply chain security policy, and monitor, evaluate and, where necessary, act upon changes in the cybersecurity practices of suppliers and service providers, at planned intervals and when significant changes to operations or risks or significant incidents related to the provision of ICT services or having impact on the security of the ICT products from suppliers and service providers occur.

5.1.7. For the purpose of point 5.1.6, the relevant entities shall:

(a) regularly monitor reports on the implementation of the service level agreements, where applicable;

(b) review incidents related to ICT products and ICT services from suppliers and service providers;

(c) assess the need for unscheduled reviews and document the findings in a comprehensible manner;

(d) analyse the risks presented by changes related to ICT products and ICT services from suppliers and service providers and, where appropriate, take mitigating measures in a timely manner.

5.2. *Directory of suppliers and service providers*

The relevant entities shall maintain and keep up to date a registry of their direct suppliers and service providers, including:

(a) contact points for each direct supplier and service provider;

(b) a list of ICT products, ICT services, and ICT processes provided by the direct supplier or service provider to the relevant entities.

6. **Security in network and information systems acquisition, development and maintenance (Article 21(2), point (e), of Directive (EU) 2022/2555)**

6.1. *Security in acquisition of ICT services or ICT products*

6.1.1. For the purpose of Article 21(2), point (e) of Directive (EU) 2022/2555, the relevant entities shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products for components that are critical for the relevant entities' security of network and information systems, based on the risk assessment carried out pursuant to point 2.1, from suppliers or service providers throughout their life cycle.

6.1.2. For the purpose of point 6.1.1, the processes referred to in point 6.1.1 shall include:

(a) security requirements to apply to the ICT services or ICT products to be acquired;

(b) requirements regarding security updates throughout the entire lifetime of the ICT services or ICT products, or replacement after the end of the support period;

(c) information describing the hardware and software components used in the ICT services or ICT products;

(d) information describing the implemented cybersecurity functions of the ICT services or ICT products and the configuration required for their secure operation;

(e) assurance that the ICT services or ICT products comply with the security requirements according to point (a);

(f) methods for validating that the delivered ICT services or ICT products are compliant to the stated security requirements, as well as documentation of the results of the validation.

6.1.3. The relevant entities shall review and, where appropriate, update the processes at planned intervals and when significant incidents occur.

6.2. *Secure development life cycle*

6.2.1. Before developing a network and information system, including software, the relevant entities shall lay down rules for the secure development of network and information systems and apply them when developing network and information systems in-house, or when outsourcing the development of network and information systems. The rules shall cover all development phases, including specification, design, development, implementation and testing.

6.2.2. For the purpose of point 6.2.1, the relevant entities shall:

(a) carry out an analysis of security requirements at the specification and design phases of any development or acquisition project undertaken by the relevant entities or on behalf of those entities;

(b) apply principles for engineering secure systems and secure coding principles to any information system development activities such as promoting cybersecurity-by-design, zero-trust architectures;

(c) lay down security requirements regarding development environments;

(d) establish and implement security testing processes in the development life cycle;

(e) appropriately select, protect and manage security test data;

(f) sanitise and anonymise testing data according to the risk assessment carried out pursuant to point 2.1.

6.2.3. For outsourced development of network and information systems, the relevant entities shall also apply the policies and procedures referred to in points 5 and 6.1.

6.2.4. The relevant entities shall review and, where necessary, update their secure development rules at planned intervals.

6.3. *Configuration management*

6.3.1. The relevant entities shall take the appropriate measures to establish, document, implement, and monitor configurations, including security configurations of hardware, software, services and networks.

6.3.2. For the purpose of point 6.3.1, the relevant entities shall:

(a) lay down and ensure security in configurations for their hardware, software, services and networks;

(b) lay down and implement processes and tools to enforce the laid down secure configurations for hardware, software, services and networks, for newly installed systems as well as for systems in operation over their lifetime.

6.3.3. The relevant entities shall review and, where appropriate, update configurations at planned intervals or when significant incidents or significant changes to operations or risks occur.

6.4. *Change management, repairs and maintenance*

6.4.1. The relevant entities shall apply change management procedures to control changes of network and information systems. Where applicable, the procedures shall be consistent with the relevant entities' general policies concerning change management.

6.4.2. The procedures referred to in point 6.4.1 shall be applied for releases, modifications and emergency changes of any software and hardware in operation and changes to the configuration. The procedures shall ensure that those changes are documented and, based on the risk assessment carried out pursuant to point 2.1, tested and assessed in view of the potential impact before being implemented.

6.4.3. In the event that the regular change management procedures could not be followed due to an emergency, the relevant entities shall document the result of the change, and the explanation for why the procedures could not be followed.

6.4.4. The relevant entities shall review and, where appropriate, update the procedures at planned intervals and when significant incidents or significant changes to operations or risks.

6.5. *Security testing*

6.5.1. The relevant entities shall establish, implement and apply a policy and procedures for security testing.

6.5.2. The relevant entities shall:

(a) establish, based on the risk assessment carried out pursuant to point 2.1, the need, scope, frequency and type of security tests;

(b) carry out security tests according to a documented test methodology, covering the components identified as relevant for secure operation in a risk analysis;

(c) document the type, scope, time and results of the tests, including assessment of criticality and mitigating actions for each finding;

(d) apply mitigating actions in case of critical findings.

6.5.3. The relevant entities shall review and, where appropriate, update their security testing policies at planned intervals.

6.6. *Security patch management*

6.6.1. The relevant entities shall specify and apply procedures, coherent with the change management procedures referred to in point 6.4.1 as well as with vulnerability management, risk management and other relevant management procedures, for ensuring that:

(a) security patches are applied within a reasonable time after they become available;

(b) security patches are tested before being applied in production systems;

(c) security patches come from trusted sources and are checked for integrity;

(d) additional measures are implemented and residual risks are accepted in cases where a patch is not available or not applied pursuant to point 6.6.2.

6.6.2. By way of derogation from point 6.6.1(a), the relevant entities may choose not to apply security patches when the disadvantages of applying the security patches outweigh the cybersecurity benefits. The relevant entities shall duly document and substantiate the reasons for any such decision.

6.7. *Network security*

6.7.1. The relevant entities shall take the appropriate measures to protect their network and information systems from cyber threats.

6.7.2. For the purpose of point 6.7.1, the relevant entities shall:

(a) document the architecture of the network in a comprehensible and up to date manner;

(b) determine and apply controls to protect the relevant entities' internal network domains from unauthorised access;

(c) configure controls to prevent accesses and network communication not required for the operation of the relevant entities;

(d) determine and apply controls for remote access to network and information systems, including access by service providers;

(e) not use systems used for administration of the security policy implementation for other purposes;

(f) explicitly forbid or deactivate unneeded connections and services;

(g) where appropriate, exclusively allow access to the relevant entities' network and information systems by devices authorised by those entities;

(h) allow connections of service providers only after an authorisation request and for a set time period, such as the duration of a maintenance operation;

(i) establish communication between distinct systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of their end points and protection of the channel data from modification or disclosure;

(j) adopt an implementation plan for the full transition towards latest generation network layer communication protocols in a secure, appropriate and gradual way and establish measures to accelerate such transition;

(k) adopt an implementation plan for the deployment of internationally agreed and interoperable modern e-mail communications standards to secure e-mail communications to mitigate vulnerabilities linked to e-mail-related threats and establish measures to accelerate such deployment;

(l) apply best practices for the security of the DNS, and for Internet routing security and routing hygiene of traffic originating from and destined to the network.

6.7.3. The relevant entities shall review and, where appropriate, update these measures at planned intervals and when significant incidents or significant changes to operations or risks occur.

6.8. *Network segmentation*

6.8.1. The relevant entities shall segment systems into networks or zones in accordance with the results of the risk assessment referred to in point 2.1. They shall segment their systems and networks from third parties' systems and networks.

6.8.2. For that purpose, the relevant entities shall:

(a) consider the functional, logical and physical relationship, including location, between trustworthy systems and services;

(b) grant access to a network or zone based on an assessment of its security requirements;

(c) keep systems that are critical to the relevant entities operation or to safety in secured zones;

(d) deploy a demilitarised zone within their communication networks to ensure secure communication originating from or destined to their networks;

(e) restrict access and communications between and within zones to those necessary for the operation of the relevant entities or for safety;

(f) separate the dedicated network for administration of network and information systems from the relevant entities' operational network;

(g) segregate network administration channels from other network traffic;

(h) separate the production systems for the relevant entities' services from systems used in development and testing, including backups.

6.8.3. The relevant entities shall review and, where appropriate, update network segmentation at planned intervals and when significant incidents or significant changes to operations or risks.

6.9. *Protection against malicious and unauthorised software*

6.9.1. The relevant entities shall protect their network and information systems against malicious and unauthorised software.

6.9.2. For that purpose, the relevant entities shall in particular implement measures that detect or prevent the use of malicious or unauthorised software. The relevant entities shall, where appropriate, ensure that their network and information systems are equipped with detection and response software, which is updated regularly in accordance with the risk assessment carried out pursuant to point 2.1 and the contractual agreements with the providers.

6.10. *Vulnerability handling and disclosure*

6.10.1. The relevant entities shall obtain information about technical vulnerabilities in their network and information systems, evaluate their exposure to such vulnerabilities, and take appropriate measures to manage the vulnerabilities.

6.10.2. For the purpose of point 6.10.1, the relevant entities shall:

(a) monitor information about vulnerabilities through appropriate channels, such as announcements of CSIRTs, competent authorities or information provided by suppliers or service providers;

(b) perform, where appropriate, vulnerability scans, and record evidence of the results of the scans, at planned intervals;

(c) address, without undue delay, vulnerabilities identified by the relevant entities as critical to their operations;

(d) ensure that their vulnerability handling is compatible with their change management, security patch management, risk management and incident management procedures;

(e) lay down a procedure for disclosing vulnerabilities in accordance with the applicable national coordinated vulnerability disclosure policy.

6.10.3. When justified by the potential impact of the vulnerability, the relevant entities shall create and implement a plan to mitigate the vulnerability. In other cases, the relevant entities shall document and substantiate the reason why the vulnerability does not require remediation.

6.10.4. The relevant entities shall review and, where appropriate, update at planned intervals the channels they use for monitoring vulnerability information.

7. **Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (Article 21(2), point (f), of Directive (EU) 2022/2555)**

7.1. For the purpose of Article 21(2), point (f) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures to assess whether the cybersecurity risk-management measures taken by the relevant entity are effectively implemented and maintained.

7.2. The policy and procedures referred to in point 7.1 shall take into account results of the risk assessment pursuant to point 2.1 and past significant incidents. The relevant entities shall determine:

(a) what cybersecurity risk-management measures are to be monitored and measured, including processes and controls;

(b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

(c) when the monitoring and measuring is to be performed;

(d) who is responsible for monitoring and measuring the effectiveness of the cybersecurity risk-management measures;

(e) when the results from monitoring and measurement are to be analysed and evaluated;

(f) who has to analyse and evaluate these results.

7.3. The relevant entities shall review and, where appropriate, update the policy and procedures at planned intervals and when significant incidents or significant changes to operations or risks.

8. **Basic cyber hygiene practices and security training (Article 21(2), point (g), of Directive (EU) 2022/2555)**

8.1. *Awareness raising and basic cyber hygiene practices*

8.1.1. For the purpose of Article 21(2), point (g) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees, including members of management bodies, as well as direct suppliers and service providers are aware of risks, are informed of the importance of cybersecurity and apply cyber hygiene practices.

8.1.2. For the purpose of point 8.1.1, the relevant entities shall offer to their employees, including members of management bodies, as well as to direct suppliers and service providers where appropriate in accordance with point 5.1.4, an awareness raising programme, which shall:

(a) be scheduled over time, so that the activities are repeated and cover new employees;

(b) be established in line with the network and information security policy, topic-specific policies and relevant procedures on network and information security;

(c) cover relevant cyber threats, the cybersecurity risk-management measures in place, contact points and resources for additional information and advice on cybersecurity matters, as well as cyber hygiene practices for users.

8.1.3. The awareness raising programme shall, where appropriate, be tested in terms of effectiveness. The awareness raising programme shall be updated and offered at planned intervals taking into account changes in cyber hygiene practices, and the current threat landscape and risks posed to the relevant entities.

8.2. *Security training*

8.2.1. The relevant entities shall identify employees, whose roles require security relevant skill sets and expertise, and ensure that they receive regular training on network and information system security.

8.2.2. The relevant entities shall establish, implement and apply a training program in line with the network and information security policy, topic-specific policies and other relevant procedures on network and information security which lays down the training needs for certain roles and positions based on criteria.

8.2.3. The training referred to in point 8.2.1 shall be relevant to the job function of the employee and its effectiveness shall be assessed. Training shall take into consideration security measures in place and cover the following:

(a) instructions regarding the secure configuration and operation of the network and information systems, including mobile devices;

(b) briefing on known cyber threats;

(c) training of the behaviour when security-relevant events occur.

8.2.4. The relevant entities shall apply training to staff members who transfer to new positions or roles which require security relevant skill sets and expertise.

8.2.5. The program shall be updated and run periodically taking into account applicable policies and rules, assigned roles, responsibilities, as well as known cyber threats and technological developments.

9. **Cryptography (Article 21(2), point (h), of Directive (EU) 2022/2555)**

9.1. For the purpose of Article 21(2), point (h) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures related to cryptography, with a view to ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of data in line with the relevant entities' asset classification and the results of the risk assessment carried out pursuant to point 2.1.

9.2. The policy and procedures referred to in point 9.1 shall establish:

(a) in accordance with the relevant entities' classification of assets, the type, strength and quality of the cryptographic measures required to protect the relevant entities' assets, including data at rest and data in transit;

(b) based on point (a), the protocols or families of protocols to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices to be approved and required for use in the relevant entities, following, where appropriate, a cryptographic agility approach;

(c) the relevant entities' approach to key management, including, where appropriate, methods for the following:

(i) generating different keys for cryptographic systems and applications;

(ii) issuing and obtaining public key certificates;

(iii) distributing keys to intended entities, including how to activate keys when received;

(iv) storing keys, including how authorised users obtain access to keys;

(v) changing or updating keys, including rules on when and how to change keys;

(vi) dealing with compromised keys;

(vii) revoking keys including how to withdraw or deactivate keys;

(viii) recovering lost or corrupted keys;

(ix) backing up or archiving keys;

(x) destroying keys;

(xi) logging and auditing of key management-related activities;

(xii) setting activation and deactivation dates for keys ensuring that the keys can only be used for the specified period of time according to the organization's rules on key management.

9.3. The relevant entities shall review and, where appropriate, update their policy and procedures at planned intervals, taking into account the state of the art in cryptography.

10. **Human resources security (Article 21(2), point (i), of Directive (EU) 2022/2555)**

10.1. *Human resources security*

10.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees and direct suppliers and service providers, wherever applicable, understand and commit to their security responsibilities, as appropriate for the offered services and the job and in line with the relevant entities' policy on the security of network and information systems.

10.1.2. The requirement referred to in point 10.1.1 shall include the following:

(a) mechanisms to ensure that all employees, direct suppliers and service providers, wherever applicable, understand and follow the standard cyber hygiene practices that the relevant entities apply pursuant to point 8.1;

(b) mechanisms to ensure that all users with administrative or privileged access are aware of and act in accordance with their roles, responsibilities and authorities;

(c) mechanisms to ensure that members of management bodies understand and act in accordance with their role, responsibilities and authorities regarding network and information system security;

(d) mechanisms for hiring personnel qualified for the respective roles, such as reference checks, vetting procedures, validation of certifications, or written tests.

10.1.3. The relevant entities shall review the assignment of personnel to specific roles as referred to in point 1.2, as well as their commitment of human resources in that regard, at planned intervals and at least annually. They shall updatethe assignment where necessary.

10.2. *Verification of background*

10.2.1. The relevant entities shall ensure to the extent feasible verification of the background of their employees, and where applicable of direct suppliers and service providers in accordance with point 5.1.4, if necessary for their role, responsibilities and authorisations.

10.2.2. For the purpose of point 10.2.1, the relevant entities shall:

(a) put in place criteria, which set out which roles, responsibilities and authorities shall only be exercised by persons whose background has been verified;

(b) ensure that verification referred to in point 10.2.1 is performed on these persons before they start exercising these roles, responsibilities and authorities, which shall take into consideration the applicable laws, regulations, and ethics in proportion to the business requirements, the asset classification as referred to in point 12.1 and the network and information systems to be accessed, and the perceived risks.

10.2.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and update it where necessary.

10.3. *Termination or change of employment procedures*

10.3.1. The relevant entities shall ensure that network and information system security responsibilities and duties that remain valid after termination or change of employment of their employees are contractually defined and enforced.

10.3.2. For the purpose of point 10.3.1, the relevant entities shall include in the individual's terms and conditions of employment, contract or agreement the responsibilities and duties that are still valid after termination of employment or contract, such as confidentiality clauses.

10.4. *Disciplinary process*

10.4.1. The relevant entities shall establish, communicate and maintain a disciplinary process for handling violations of network and information system security policies. The process shall take into consideration relevant legal, statutory, contractual and business requirements.

10.4.2. The relevant entities shall review and, where appropriate, update the disciplinary process at planned intervals, and when necessary due to legal changes or significant changes to operations or risks.

11. **Access control (Article 21(2), points (i) and (j), of Directive (EU) 2022/2555)**

11.1. *Access control policy*

11.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall establish, document and implement logical and physical access control policies for the access to their network and information systems, based on business requirements as well as network and information system security requirements.

11.1.2. The policies referred to in point 11.1.1. shall:

(a) address access by persons, including staff, visitors, and external entities such as suppliers and service providers;

(b) address access by network and information systems;

(c) ensure that access is only granted to users that have been adequately authenticated.

11.1.3. The relevant entities shall review and, where appropriate, update the policies at planned intervals and when significant incidents or significant changes to operations or risks occur.

11.2. *Management of access rights*

11.2.1. The relevant entities shall provide, modify, remove and document access rights to network and information systems in accordance with the access control policy referred to in point 11.1.

11.2.2. The relevant entities shall:

(a) assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;

(b) ensure that access rights are modified accordingly upon termination or change of employment;

(c) ensure that access to network and information systems is authorised by the relevant persons;

(d) ensure that access rights appropriately address third-party access, such as visitors, suppliers and service providers, in particular by limiting access rights in scope and in duration;

(e) maintain a register of access rights granted;

(f) apply logging to the management of access rights.

11.2.3. The relevant entities shall review access rights at planned intervals and shall modify them based on organisational changes. The relevant entities shall document the results of the review including the necessary changes of access rights.

11.3. *Privileged accounts and system administration accounts*

11.3.1. The relevant entities shall maintain policies for management of privileged accounts and system administration accounts as part of the access control policy referred to in point 11.1.

11.3.2. The policies referred to in point 11.3.1 shall:

(a) establish strong identification, authentication such as multi-factor authentication, and authorisation procedures for privileged accounts and system administration accounts;

(b) set up specific accounts to be used for system administration operations exclusively, such as installation, configuration, management or maintenance;

(c) individualise and restrict system administration privileges to the highest extent possible,

(d) provide that system administration accounts are only used to connect to system administration systems.

11.3.3. The relevant entities shall review access rights of privileged accounts and system administration accounts at planned intervals and be modified based on organisational changes, and shall document the results of the review, including the necessary changes of access rights.

11.4. *Administration systems*

11.4.1. The relevant entities shall restrict and control the use of system administration systems in accordance with the access control policy referred to in point 11.1.

11.4.2. For that purpose, the relevant entities shall:

(a) only use system administration systems for system administration purposes, and not for any other operations;

(b) separate logically such systems from application software not used for system administrative purposes,

(c) protect access to system administration systems through authentication and encryption.

11.5. *Identification*

11.5.1. The relevant entities shall manage the full life cycle of identities of network and information systems and their users.

11.5.2. For that purpose, the relevant entities shall:

(a) set up unique identities for network and information systems and their users;

(b) link the identity of users to a single person;

(c) ensure oversight of identities of network and information systems;

(d) apply logging to the management of identities.

11.5.3. The relevant entities shall only permit identities assigned to multiple persons, such as shared identities, where they are necessary for business or operational reasons and are subject to an explicit approval process and documentation. The relevant entities shall take identities assigned to multiple persons into account in the cybersecurity risk management framework referred to in point 2.1.

11.5.4. The relevant entities shall regularly review the identities for network and information systems and their users and, if no longer needed, deactivate them without delay.

11.6. *Authentication*

11.6.1. The relevant entities shall implement secure authentication procedures and technologies based on access restrictions and the policy on access control.

11.6.2. For that purpose, the relevant entities shall:

(a) ensure the strength of authentication is appropriate to the classification of the asset to be accessed;

(b) control the allocation to users and management of secret authentication information by a process that ensures the confidentiality of the information, including advising personnel on appropriate handling of authentication information;

(c) require the change of authentication credentials initially, at predefined intervals and upon suspicion that the credentials were compromised;

(d) require the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-in attempts;

(e) terminate inactive sessions after a predefined period of inactivity; and

(f) require separate credentials to access privileged access or administrative accounts.

11.6.3. The relevant entities shall to the extent feasible use state-of-the-art authentication methods, in accordance with the associated assessed risk and the classification of the asset to be accessed, and unique authentication information.

11.6.4. The relevant entities shall review the authentication procedures and technologies at planned intervals.

11.7. *Multi-factor authentication*

11.7.1. The relevant entities shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms for accessing the relevant entities' network and information systems, where appropriate, in accordance with the classification of the asset to be accessed.

11.7.2. The relevant entities shall ensure that the strength of authentication is appropriate for the classification of the asset to be accessed.

12. **Asset management (Article 21(2), point (i), of Directive (EU) 2022/2555)**

12.1. *Asset classification*

12.1.1. For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall lay down classification levels of all assets, including information, in scope of their network and information systems for the level of protection required.

12.1.2. For the purpose of point 12.1.1, the relevant entities shall:

(a) lay down a system of classification levels for assets;

(b) associate all assets with a classification level, based on confidentiality, integrity, authenticity and availability requirements, to indicate the protection required according to their sensitivity, criticality, risk and business value;

(c) align the availability requirements of the assets with the delivery and recovery objectives set out in their business continuity and disaster recovery plans.

12.1.3. The relevant entities shall conduct periodic reviews of the classification levels of assets and update them, where appropriate.

12.2. *Handling of assets*

12.2.1. The relevant entities shall establish, implement and apply a policy for the proper handling of assets, including information, in accordance with their network and information security policy, and shall communicate the policy on proper handling of assets to anyone who uses or handles assets.

12.2.2. The policy shall:

(a) cover the entire life cycle of the assets, including acquisition, use, storage, transportation and disposal;

(b) provide rules on the safe use, safe storage, safe transport, and the irretrievable deletion and destruction of the assets;

(c) provide that the transfer shall take place in a secure manner, in accordance with the type of asset to be transferred.

12.2.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.

12.3. *Removable media policy*

12.3.1. The relevant entities shall establish, implement and apply a policy on the management of removable storage media and communicate it to their employees and third parties who handle removable storage media at the relevant entities' premises or other locations where the removable media is connected to the relevant entities' network and information systems.

12.3.2. The policy shall:

(a) provide for a technical prohibition of the connection of removable media unless there is an organisational reason for their use;

(b) provide for disabling self-execution from such media and scanning the media for malicious code before they are used on the relevant entities' systems;

(c) provide measures for controlling and protecting portable storage devices containing data while in transit and in storage;

(d) where appropriate, provide measures for the use of cryptographic techniques to protect data on removable storage media.

12.3.3. The relevant entities shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.

12.4. *Asset inventory*

12.4.1. The relevant entities shall develop and maintain a complete, accurate, up-to-date and consistent inventory of their assets. They shall record changes to the entries in the inventory in a traceable manner.

12.4.2. The granularity of the inventory of the assets shall be at a level appropriate for the needs of the relevant entities. The inventory shall include the following:

(a) the list of operations and services and their description,

(b) the list of network and information systems and other associated assets supporting the relevant entities' operations and services.

12.4.3. The relevant entities shall regularly review and update the inventory and their assets and document the history of changes.

12.5. *Deposit, return or deletion of assets upon termination of employment*

The relevant entities shall establish, implement and apply procedures which ensure that their assets which are under custody of personnel are deposited, returned or deleted upon termination of employment, and shall document the deposit, return and deletion of those assets. Where the deposit, return or deletion of assets is not possible, the relevant entities shall ensure that the assets can no longer access the relevant entities' network and information systems in accordance with point 12.2.2.

13. **Environmental and physical security (Article 21(2), points (c), (e) and (i) of Directive (EU) 2022/2555)**

13.1. *Supporting utilities*

13.1.1. For the purpose of Article 21(2)(c) of Directive (EU) 2022/2555, the relevant entities shall prevent loss, damage or compromise of network and information systems or interruption to their operations due to the failure and disruption of supporting utilities.

13.1.2. For that purpose, the relevant entities shall, where appropriate:

(a) protect facilities from power failures and other disruptions caused by failures in supporting utilities such as electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning;

(b) consider the use of redundancy in utilities services;

(c) protect utility services for electricity and telecommunications, which transport data or supply network and information systems, against interception and damage;

(d) monitor the utility services referred to in point (c) and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point 13.2.2(b) affecting the utility services;

(e) conclude contracts for the emergency supply with corresponding services, such as for the fuel for emergency power supply;

(f) ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.

13.1.3. The relevant entities shall test, review and, where appropriate, update the protection measures on a regular basis or following significant incidents or significant changes to operations or risks.

13.2. *Protection against physical and environmental threats*

13.2.1. For the purpose of Article 21(2)(e) of Directive (EU) 2022/2555, the relevant entities shall prevent or reduce the consequences of events originating from physical and environmental threats, such as natural disasters and other intentional or unintentional threats, based on the results of the risk assessment carried out pursuant to point 2.1.

13.2.2. For that purpose, the relevant entities shall, where appropriate:

(a) design and implement protection measures against physical and environmental threats;

(b) determine minimum and maximum control thresholds for physical and environmental threats;

(c) monitor environmental parameters and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point (b).

13.2.3. The relevant entities shall test, review and, where appropriate, update the protection measures against physical and environmental threats on a regular basis or following significant incidents or significant changes to operations or risks.

13.3. *Perimeter and physical access control*

13.3.1. For the purpose of Article 21(2)(i) of Directive (EU) 2022/2555, the relevant entities shall prevent and monitor unauthorised physical access, damage and interference to their network and information systems.

13.3.2. For that purpose, the relevant entities shall:

(a) on the basis of the risk assessment carried out pursuant to point 2.1, lay down and use security perimeters to protect areas where network and information systems and other associated assets are located;

(b) protect the areas referred to in point (a) by appropriate entry controls and access points;

(c) design and implement physical security for offices, rooms and facilities,

(d) continuously monitor their premises for unauthorised physical access.

13.3.3. The relevant entities shall test, review and, where appropriate, update the physical access control measures on a regular basis or following significant incidents or significant changes to operations or risks.