



Brussels, 19.1.2026
C(2026) 413 final

Standard under Commission Decision (EU, Euratom) 2017/46

Security rules for outsourced systems

TABLE OF CONTENTS

1.	Introduction	2
2.	Scope and definitions.....	3
3.	Context and risks	3
	Institutional independence and data sovereignty	3
	Lock-in	4
	Responsibility sharing	4
	Heterogeneity of outsourcing	5
	Encryption of information	5
4.	Compliance obligations	5
	Corporate IT governance and security rules.....	6
	Appropriate processes and oversight.....	6
	Rules on personal data protection, AI and digital markets.....	7
	Verification procedure.....	7
5.	Security rules for outsourced systems	7
	Rule 1: Commission information must be hosted within the EU	8
	Rule 2: Legal and technical requirements and conditions for the protection of information must be included in outsourcing contracts.....	8
	Rule 3: Commission information must be isolated from other customers' information	8
	Rule 4: Identity verification, authentication, authorisation mechanisms and credentials must be controlled by the Commission	9
	Rule 5: The availability of Commission information must be ensured	9
	Rule 6: A security incident response procedure must be put in place	10
	Rule 7: The Commission must be able to check the security logs of its outsourced systems and services.....	11
	Rule 8: Outsourced systems must apply the zero-trust principle.....	11
	Rule 9: The encryption keys used to encrypt SNC information must remain under the Commission's control	12
	Rule 10: Access to Commission information by service provider staff must be minimised .	13
	Rule 11: Continuous improvement of the security of outsourced systems.....	13
	Rule 12: Compliance, audit and penetration testing	14
6.	Contact points	14

1. INTRODUCTION

This standard outlines the mandatory security rules for outsourced information systems of the European Commission. Its aim is to protect Commission information by laying down clear requirements for information system owners and outsourcing providers and by specifying their responsibilities. It complements Commission Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission ⁽¹⁾ and its implementing rules.

This standard replaces the previous standard of 2020 ⁽²⁾ and reflects the changed international threat landscape and the wider use of outsourcing at the Commission. It responds to the need to increase the Commission's resilience and independence in line with the report *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness* and the need to ensure security by design and by default ⁽³⁾. Outsourcing carries specific risks, such as data exposure, provider lock-in and the risks associated with sharing responsibility for security and risks associated with high-risk providers ⁽⁴⁾. This document provides a framework for mitigating these risks and ensuring that outsourced systems meet the Commission's security requirements and are in line with the relevant EU regulations, including the Cyber Security Act, the Cyber Resilience Act, Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, the Network and Information Security Directive 2 (NIS 2) and the Digital Operational Resilience Act (DORA) ⁽⁵⁾. If the outsourcing concerns processing of personal data, Regulation (EU) 2018/1725 (EUDPR) sets specific requirements as to the content of an agreement with the provider and the processing itself.

The Commission must be able to deter and neutralise attacks to ensure the continuity of its core activities, resilience and data sovereignty. This can only be done if it and its outsourcing providers cooperate closely on information security and if security measures are implemented by design and by default.

2. SCOPE AND DEFINITIONS

Article 8 of Decision (EU, Euratom) 2018/559 defines outsourcing as follows.

“A Commission system is outsourced when it is provided under a contract with a third-party contractor and is hosted on non-Commission premises. This includes the outsourcing

⁽¹⁾ Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

⁽²⁾ C(2020) 4190 final.

⁽³⁾ Security by design means building systems with security as a foundational requirement, not as an afterthought. Security by default means configuring systems so they are secure out of the box, without requiring the user to take extra steps.

⁽⁴⁾ Exposure to high-risk suppliers from third countries can create a risk of foreign interference.

⁽⁵⁾ Many of the EU's digital policies do not directly apply to the Commission; they are, however, applicable to its outsourcing providers.

of IT services, data centres and the processing of Commission data sets by external services.”

The mandatory security rules apply to:

- (i) private and public cloud services, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) projects ⁽⁶⁾;
- (ii) service contracts whose execution involves the processing of Commission information and requires an outsourced IT system to do so;
- (iii) outsourced data processing or storage components of an information system;
- (iv) services provided at no cost and approved for use in the Commission, for instance an artificial intelligence (AI) chatbot or internet solutions;
- (v) outsourced system environments, including production, test and development systems and backups.

3. CONTEXT AND RISKS

Institutional independence and data sovereignty

Outsourcing business processes, including the processing of information, comes with several constraints and risks, which must be accepted at the appropriate management level before a decision to outsource is taken. The independence of the European Commission needs to be guaranteed.

Article 17(3) of the Treaty on European Union states: “the Commission shall be completely independent. Without prejudice to Article 18(2), the members of the Commission shall neither seek nor take instructions from any Government or other institution, body, office or entity.”

This has several consequences for outsourcing:

- system owners must make sure that any outsourcing decision they take does not compromise the independence of the operations and the governance of the Commission;
- system owners must avoid becoming dependent on services that are susceptible to interference from companies and/or non-EU countries that do not fully comply with the EU legal framework, that carry out malicious cyber activities or that can otherwise compromise its independence, unless there is no other service available and the risk is accepted at senior management level;
- system owners must also be aware of and, where possible, avoid dependency on entities with a potential conflict of interests with the Commission.

⁽⁶⁾ Maintaining detailed guidelines regarding IaaS, PaaS and SaaS and private cloud architectures is the responsibility of the Commission’s internal Cloud Council.

Where concerns arise as to possible interference by companies or non-EU countries when using an outsourced service provider, such risk must be documented by the system owner in the project charter and reviewed by the Commission's Information Technology and Cybersecurity Board, taking account of the Sovereignty Score of services ⁽⁷⁾, where available. The Directorate-General for Digital Services (DG DIGIT) supports system owners in implementing outsourcing solutions compatible with the independence of the Commission.

Lock-in

Lock-in occurs when a customer is dependent on a specific provider for products or services and unable to use another provider without incurring significant switching costs. Outsourcing implies a certain degree of lock-in. Without proper contractual safeguards and exit planning, the Commission risks losing access to its information, customisations, integrations, historical analytics and proprietary configurations developed within the provider's environment.

Choosing open-source and standard-based products and services while maintaining some internal and backup capability and capacity may reduce the risk of lock-in and facilitate reversibility.

Responsibility sharing

System owners must seek binding commitments in contracts with providers on the sharing of responsibilities to ensure confidentiality, availability and information integrity. System owners must document and implement the security measures under their responsibility ⁽⁸⁾.

For their part, providers must acknowledge and commit themselves to implementing their responsibilities under the shared responsibility model ⁽⁹⁾. Providers must agree to manage and secure the Commission's information and commit to implementing auditable security practices and contractual safeguards. However, system owners should be aware that the Commission remains responsible for managing the risks associated with its information even when the management of some risks is transferred to the provider in question.

Third-party assessments and certifications at national or EU level can be used to assure that the provider implements best practices and the applicable cybersecurity rules and regulations.

Heterogeneity of outsourcing

Each outsourcing case is unique due to the variety of outsourcing projects and activities in the Commission. The application of the IT security framework and of the outsourcing rules

⁽⁷⁾ DG DIGIT provided a sovereignty score to be used in the evaluation of outsourcing projects, Cloud Sovereignty Framework, October 2025.

⁽⁸⁾ This may include drawing up RASCI matrices showing the roles and responsibilities of the various stakeholders in the supply chain and embedding these in contracts with suppliers, as well as implementing the relevant standards (for instance ISO 27017 and ISO 27018 requirements for cloud security management).

⁽⁹⁾ Key responsibilities of the provider typically include Physical security, Infrastructure security, Network security and virtualisation, and can expand to other domains. Providers must ensure observability and transparency of their activities.

set out below requires a careful risk assessment to enable business owners to take informed decisions.

DG DIGIT is the main broker for outsourced cloud services. In general, using outsourcing providers recommended by DG DIGIT is more cost-effective, reduces overall risk and makes it easier to assess risks.

Even if a system owner opts not to use DG DIGIT's services, they must consult DG DIGIT to ensure compliance with this standard if an outsourcing project involves an IT component. DG DIGIT manages framework contracts with the main service and cloud providers that include a secure landing zone ⁽¹⁰⁾ and high- and low-level security controls, helping system and data owners meet the requirements of this standard.

Encryption of information

Depending on the type of service and the available encryption features, encryption can offer various levels of protection against unauthorised access to Commission information. While in most cases encryption reduces the attack surface, all encryption technologies and architecture types have their weaknesses, especially if unencrypted metadata is considered. Specifically, system owners must ensure that their systems implement post-quantum cryptographic (PQC) algorithms, in line with the Commission's PQC transition plan.

4. COMPLIANCE OBLIGATIONS

Compliance with these rules does not exempt system owners from applying other requirements of the Commission's information security policy ⁽¹¹⁾. This section provides a non-exhaustive overview of obligations stemming from EU legislation and from the Commission's IT security and cybersecurity policy ⁽¹²⁾. System owners must assess the confidentiality, integrity and availability of their information and assign it to one of the following four categories.

- **Publicly available (PA) information:** information that is intended to be or already has been, released to the public.
- **Commission use (CU) information:** normal, working-level information used inside the Commission. This information is not particularly sensitive, but it is still covered by Article 17 of the Staff Regulations. It is therefore not considered to be publicly available.
- **Sensitive non-classified (SNC) information:** information or material that the Commission must protect because of legal obligations laid down in the Treaties or in acts adopted in implementing them, or because its unauthorised disclosure could cause harm to the interests or reputation of the European Union or its

⁽¹⁰⁾ A secure landing zone in the cloud is a pre-configured governed environment that provides a baseline for deploying workloads securely and efficiently.

⁽¹¹⁾ Including the relevant corporate guidance and best practice requirements.

⁽¹²⁾ See Commission Decision (EU, Euratom) 2017/46, Commission Decision (EU, Euratom) 2015/443 and in the security notices C(2019) 1903 and C(2019) 1904.

Member States and third parties, such as businesses and companies or private individuals.

- **EU classified information:** any information or material with ‘classified’ status accorded in line with the EU security classification rules. The outsourcing of such information must be approved by the Commission Security Authority established under Decision (EU, Euratom) 2015/444.

Corporate IT governance and security rules

The Commission remains responsible for the governance and security of its information, and this responsibility cannot be outsourced. System owners must:

- (i) declare any outsourcing in GovIS2, even if it concerns a component of an information system;
- (ii) address associated risks in a security and business continuity plan;
- (iii) put the control mechanisms set out in those plans in place in a timely manner; and
- (iv) assess compliance with the IT security policy and the rules listed in this standard using the governance, risk and compliance (GRC) compliance workflows.

The same applies when an outsourced system is used as part of a service contract whose primary objective is not the purchase of such a system, but the delivery of business functions based on information processing.

Appropriate processes and oversight

The outsourcing of ICT systems requires a series of baseline requirements and processes to be put in place between the system owner and the provider for the implementation of a shared security oversight model. The most important of these processes, which must be established in accordance with the rules set out in section 5, are:

- information security risk management;
- information security incident management;
- business continuity and recovery management (including backups);
- security and business continuity testing and exercising;
- vulnerability and patch management;
- compliance and audit management;
- security awareness and training;
- data encryption and data protection;
- access control and identity management;
- change and configuration management;
- appropriate threat detection and threat landscape awareness;
- security log management, and
- security monitoring.

Under the Commission's IT security policy, appropriate oversight from senior and middle management must be in place for security processes in all outsourcing contracts.

Rules on personal data protection, AI and digital markets

Due consideration should be given to the protection of personal data in line with Regulation (EU) 2018/1725 and to the safe use of AI. This equally applies to all personal data potentially used in a system's operation or to control access to it, including security and system logs. Particular attention must be paid to the potential transmission and transfer by the providers of personal data to third parties and to possible leaks in the context of AI training or fine-tuning. For the processing of sensitive non-classified (SNC) information by an AI technology in the system, a specific security standard ⁽¹³⁾ must be complied with.

Verification procedure

As part of its security inspection framework, the Security Directorate of DG Human Resources & Security (HR.DS) will verify whether the rules set out in this document have been complied with. At least once a year, HR.DS will select a sample of outsourced systems and check whether the rules have been implemented correctly. If HR.DS identifies significant risks, it will report these to the Information Technology and Cybersecurity Board.

As part of its responsibilities under Decision (EU, Euratom) 2017/46, DG DIGIT may also assess the implementation of security controls in place for outsourced systems.

5. SECURITY RULES FOR OUTSOURCED SYSTEMS

The rules set out below form part of the Commission's binding IT security policy. System owners are responsible for ensuring compliance with these rules when their systems or services are not hosted and managed by DG DIGIT. Assessment grids and training courses will be available to help system owners comply with the rules.

This standard applies to all outsourced systems, including those currently in production or development. For existing systems that do not fully comply with these rules, Commission departments may adopt a flexible approach based on a risk assessment. This assessment must evaluate:

- **Impact:** The risk to information security, Commission operations and corporate governance.
- **Remediation:** The feasibility of bringing the system into compliance.
- **Alternatives:** The possibility of migrating to a different outsourcing provider.

Commission departments should consult DG DIGIT and HR.DS for advice.

⁽¹³⁾ Standard under Commission Decision (EU, Euratom) 2017/46 Security of sensitive non-classified information in AI system, C(2025) 3738 final.

HR.DS will provide specific guidelines to assist services with the implementation of these rules for existing systems.

Rule 1: Commission information must be hosted within the EU

Publicly available information must be stored, processed and managed within the EU if the service supports essential or important functions of the Commission.

Commission use and SNC information ⁽¹⁴⁾ must be stored, processed and managed within the EU by outsourcing providers who are established in the EU and subject to the exclusive jurisdiction of a Member State. Information flows must be assessed carefully, with particular attention being paid to globally distributed storage, content delivery networks or protocol accelerators or any other scheme that might decrypt and re-encrypt information in nodes outside the EU. Such nodes may only be used if they comply strictly with the rules set out in this document. For SNC information systems, supporting essential or important functions related to the Commission's decision-making, budget execution and activities within its exclusive competence, as well as for shared-competence activities in the fields of trade, energy, defence and external action, only providers that are not subject to legal, regulatory or political interference from non-EU countries shall be used, unless the confidentiality and availability of information can be ensured by other means.

The outsourcing of SNC systems to high-risk suppliers, including providers presenting unacceptable supply-chain or jurisdictional risks, is prohibited.

Rule 2: Legal and technical requirements and conditions for the protection of information must be included in outsourcing contracts

System owners must ensure that the relevant requirements for outsourcing including the rules of this standard are reflected in binding contracts with the outsourcing provider. For contracts with an outsourcing provider, contract templates developed by DG DIGIT and by the Directorate-General for Budget (DG BUDG) must be used. At the very least, the relevant terms relating to the protection of information and personal data in the contract templates must be replicated in outsourcing contracts. Any contractual terms imposed by the provider must be examined closely to verify their compatibility with Commission rules.

The contract must clearly set out the responsibilities of, respectively, the system owner and of the service provider, as well as the shared responsibilities, if any.

Rule 3: Commission information must be isolated from other customers' information

Within a service or a component provided by a cloud service provider, Commission information must be isolated from other customers' information. System owners must obtain assurance from outsourcing providers on the physical and logical measures implemented to ensure isolation. It is strongly recommended to use encryption to improve data isolation and minimise the provider's access to Commission information. The customer management infrastructure of outsourcing providers is often shared between multiple customers. This could affect the isolation of Commission information.

⁽¹⁴⁾ This includes logs and metadata when they include Commission information or when they can be used to rebuild SNC information, identity and access control-related information, encryption keys and the hardware hosting the information.

Isolation measures must be documented in an IT security plan ⁽¹⁵⁾. Tests and/or third-party reports proving that Commission information is correctly isolated must be available, covering all levels (hosting, network, infrastructure, virtualisation, code and application).

Rule 4: Identity verification, authentication, authorisation mechanisms and credentials must be controlled by the Commission

All credentials must remain under the sole control of the Commission.

Identity assurance of privileged and other sensitive users must be verified through trusted and EU-accredited providers, in line with recognised regulatory or industry standards (e.g. Regulation 910/2014 for electronic identification, authentication and trust services). The use of unverified or isolated identity sources is not allowed.

Authentication management for outsourced systems, including SaaS and platform apps excluding emergency access accounts for security services, shall be centrally governed and based on strong, standards-based methods appropriate to the level of risk. The Commission-federated and corporate authentication services ⁽¹⁶⁾ must be used to ensure consistency and minimise risks.

Access rights (authorisation control) shall be defined and managed according to the principle of least privilege and segregation of duties. Authorisation processes should ensure that access rights remain aligned with approved organisational roles and access policies. The Commission-federated corporate authorisation service must be used to ensure consistency and minimise risks ⁽¹⁷⁾. All identity and access events shall be logged, monitored and reviewed through federated and corporate logging services to support auditability, anomaly detection and protection of information assets (accountability and traceability).

Rule 5: The availability of Commission information must be ensured

Lock-in situations affecting the availability of Commission information must be avoided. System owners must prepare adequate measures to ensure that information and systems supporting essential or important functions remain available for normal business activities in case of a failure of the outsourcing partner a unilateral cancellation of the contract or unilateral restriction of use by the contractor ⁽¹⁸⁾.

System owners must ensure that business continuity/disaster recovery plans with details on reversibility, continuity and recovery objectives and their achievement in the context of the outsourced information system are available, taking into the business requirements and associated risks. The plans must describe how service-level agreements (SLAs) signed with the various outsourcing parties involved in the provision of the service in question achieve the continuity and disaster recovery objectives and implement, in a comprehensive manner, the respective responsibilities of the parties involved, including the system owner.

⁽¹⁵⁾ DG DIGIT provides standard services for system owners to be able to implement data isolation in the context of infrastructure as a service (IaaS) and platform as a service (PaaS).

⁽¹⁶⁾ Unless duly justified, this must be the EULogin service.

⁽¹⁷⁾ Unless duly justified, this must be the EUAccess service.

⁽¹⁸⁾ The residual risks related to unlikely business continuity scenario must be documented, covering contractual and geopolitical issues.

The plans must contain or refer to SLAs' standard operating procedures for continuity and recovery, exercises and reports covering the controls introduced by outsourcing providers for network protection and load balancing ⁽¹⁹⁾.

Lock-in may affect the availability of information. A lock-in mitigation and information reversibility plan ⁽²⁰⁾ must therefore be available for review.

Rule 6: A security incident response procedure must be put in place

The service provider must report to the Commission any cybersecurity incident occurring within the outsourced service with a potential impact on the Commission. This is to ensure that the Commission can analyse and assess these incidents with the assistance of the service provider. It is crucial that the service provider commits to full transparency and cooperation, sharing any information that aids to better protect the Commission's information.

The service provider must adhere to the measures established in Decision (EU, Euratom) 2017/46 and its implementing rules. Furthermore, the following complementary provisions apply:

1. Incident response procedure: The contract must provide an incident response procedure that clearly specifies the communication channels for incidents to be used by the Commission and the service provider to report incidents. It must be possible to integrate the procedure into the Commission's existing incident response processes and capabilities.

2. Security points of contact: Both the outsourcing provider and the Commission must identify security points of contact. It is essential that the Cyber Security Incident Response Capability (CSIRC), reachable at EC-DIGIT-CSIRC@ec.europa.eu, is designated as one of these contact points.

3. Incident reporting commitment: The service provider must report immediately any security incidents and alerts affecting Commission information to CSIRC at EC-DIGIT-CSIRC@ec.europa.eu and provide regular updates to the Commission, as well as incident reports and detailed post incident reviews. The provider shall also inform the relevant system owners and security officers.

4. Disclosure coordination: The service provider must support the Commission in the regulated disclosure of breaches involving Commission information and activities to relevant regulatory authorities. In case of processing of personal data, it must be ensured that the Commission is in position to meet the specific requirements

⁽¹⁹⁾ Depending on the requirements, business continuity and reversibility may only be achieved by combining the services of several service providers, to ensure continuity of service in the event of a technical failure on the part of one of the providers.

⁽²⁰⁾ Reversibility is the degree to which cloud-based applications are designed in a way that enables them to be moved/ported to other cloud providers and/or environments. Reversibility is often easier to implement in contexts where the Commission implements standard-based solutions and open-source-/open-data-compatible services. At a minimum, a backup of SNC information must be available independently of the service provider in question. The lock-in mitigation/information reversibility plan can be part of the security plan. This plan, in turn, can be part of the continuity and disaster recovery plan.

concerning personal data breaches (Regulation (EU) 2018/1725, Articles 34-35 and the related applicable internal procedures).

Rule 7: The Commission must be able to check the security logs of its outsourced systems and services

Security logs and events from outsourced systems and services must remain accessible to the Commission at all times, including in the event of a service provider failure. Those security logs should be stored in an adequate infrastructure to protect them against tampering. Where technically feasible, the service provider should be connected to DG DIGIT's centralised monitoring, log management and security incident detection systems.

If logs are missing or if errors occur in the service provider's log synchronisation mechanism, the Commission must be informed through the established security points of contact (see Rule 6). The Commission must be able to verify the accuracy and integrity of the log content, through electronic signing or an equivalent mechanism.

Rule 8: Outsourced systems must apply the zero-trust principle

In line with the zero-trust principle, no system or resource is to be trusted by default. Every access must be explicitly specified, verified and enforced. Users and applications must be granted only the minimum connections they need, and all traffic in transit must be encrypted and filtered – at both network and application levels – through firewalls, access controls and end-to-end encryption.

Privileged access, whether by humans (such as administrators) or machines (such as application programming interfaces), is only permitted if mediated through secure gateways and preferably using Commission controlled infrastructure and devices ⁽²¹⁾. Permanent or shared credentials are strictly prohibited.

Connections to external systems must follow DG DIGIT's baseline interconnection channels and framework contracts. Any exception requires approval from HR.DS and a formal interconnection security agreement.

Finally, owners of outsourced systems must maintain detailed security documentation covering endpoints, device inventories, encryption parameters and privileged access workflows. They must implement regular reviews and audits to ensure the fulfilment of zero-trust, device-trust and privileged access management requirements.

Rule 9: The encryption keys used to encrypt SNC information must remain under the Commission's control

System owners must enforce the need-to-know principle for SNC information. Encryption is mandatory in outsourced systems to prevent third-party access to Commission information, in compliance with the Commission's cryptographic standards and post-quantum cryptography transition plan ⁽²²⁾.

⁽²¹⁾ Privileged access credentials must be centrally managed: stored in vaults, proxied, rotated, and issued as short-lived, just-in-time secrets.

⁽²²⁾ A draft standard is available for consultation and should be formally adopted by the end of 2025.

Encryption at rest and in transit is mandatory for outsourced systems processing SNC information and it is recommended for all systems. If encrypted information is stored persistently, key escrow procedures must be available ⁽²³⁾.

For outsourced systems handling SNC information, the Commission shall ensure that the service provider's access to data in cleartext is minimised. This should be achieved through encryption during processing (Confidential Computing) where available. If not available, the system owner must document the risk and implement compensating controls to ensure equivalent protection ⁽²⁴⁾.

Any key management system protecting SNC information must remain under the exclusive control of the Commission and be shielded from foreign laws with extraterritorial effects. Key generation and storage must use equipment certified in accordance with national or EU standards.

System owners must document encryption practices for information at rest, in transit and during processing. This documentation must detail the key lifecycle, including key generation, storage, escrow (if applicable) and the encryption and hashing algorithms used. The IT security plan and corresponding SLA for outsourced workloads must address the following:

- clear division of responsibilities;
- key usage control and auditing;
- runtime protection;
- key revocation strategy;
- exit and portability measures;
- policy binding and regulatory compliance.

For SNC-related outsourced workloads, the provider in question must support Hold Your Own Key (HYOK) encryption (where primary keys never leave Commission premises) or Bring Your Own Key (BYOK) encryption (where Commission-generated keys are imported into the cloud provider's hardware security models). If the cloud provider needs to generate/store keys or process unencrypted information, a formal exemption request must be submitted to the Information Technology and Cybersecurity Board via HR.DS, together with a risk assessment approved by the system owner.

Any non-standard encryption use ⁽²⁵⁾ in outsourced systems requires the approval of the Commission's Crypto Approval Authority (HR.DS).

⁽²³⁾ Key escrow is a security mechanism in which encryption keys are held in escrow – i.e. stored securely by a trusted third party (or parties) – to allow access to encrypted information under certain predefined conditions.

⁽²⁴⁾ This requirement will be updated to take account of the rules of the EU Cybersecurity Certification Scheme for cloud services, once the scheme has been adopted. In the meantime, please follow advice and guidance from the Cloud Council on the sovereignty of various solutions.

⁽²⁵⁾ As defined in the HR.DS crypto standard.

Rule 10: Access to Commission information by service provider staff must be minimised

All access by service provider staff to Commission information must be strictly controlled, time-limited, limited in scope and fully logged and documented and must comply with the following principles.

1. Least privilege and segregation of duties: Grant only the rights needed for each job. Any ‘privileged’ role (maintenance, support, emergency) must comprise only the basic functions and limited in duration.

2. EU-based and screened or security-cleared staff: Any cloud service provider handling SNC information supporting essential or important functions must use staff located in the EU and security-cleared or at minimum security-screened by national authorities. Global ‘follow-the-sun’ centres must not be given access to SNC information.

3. Identity governance and administration: System owners must implement identity governance and administration processes. If it is available, system owners should be required to use the Commission’s identity governance and administration portal ⁽²⁶⁾ to manage users’ specific roles and time windows, approval workflows, just-in-time credentials, auto-revocation and logging.

Rule 11: Continuous improvement of the security of outsourced systems

The cybersecurity threat landscape is continuously changing ⁽²⁷⁾, with most systems built around a continuous integration/continuous delivery (CI/CD) pipeline to adapt to changing business requirements, technology developments and new security risks. The outsourcing provider manages the CI/CD and associated security risks in most outsourced systems ⁽²⁸⁾.

System owners must implement security by design and by default. In case the CI/CD pipeline is under the responsibility of the Commission, they must ensure that the CI/CD pipeline includes the continuous improvement of security and regular security testing and auditing. Risky deployments must be blocked as early as possible in CI/CD pipelines, as this is the cheapest and most efficient way to ensure security by design and by default. In case the CI/CD pipeline is not visible to the Commission, audit reports regarding service providers shall cover the CI/CD maturity and security.

For systems developed under the responsibility of the Commission, managed services provided by DG DIGIT must be used to ensure the security of the CI/CD pipeline.

Rule 12: Compliance, audit and penetration testing

The results of all security audits as well as all risk, compliance, certification and penetration tests conducted by service providers must be available to the Commission and

⁽²⁶⁾ Currently being developed.

⁽²⁷⁾ In large-scale internet-based cloud environments, vulnerability or misconfiguration can be exploited in seconds, minutes or hours compared to the days, weeks or months needed in other environments.

⁽²⁸⁾ [OWASP Top 10 CI/CD Security Risks|OWASP Foundation](#).

must be regularly updated throughout the duration of the contract²⁹. Evidence of compliance with general and sectoral EU legislation (the General Data Protection Regulation, the AI Act, the Cybersecurity Act, the Cyber Solidarity Act, the Digital Services Act/Digital Markets Act, the Network and Information Security Directive 2 etc.) and standard audit reports, such as SOC-2 or BSI C5 reports (³⁰) must be available.

Security, business continuity and disaster recovery plans, including risk and impact assessments and associated role/resource provisioning, must also be made available to the Commission. The plans must make provision for reporting on the status and the effectiveness of the security, continuity and recovery controls contained in the plans and on any plans for their improvement.

System owners must also carry out a yearly penetration test of systems handling SNC information and a penetration test of Commission use systems every three years, covering all their responsibilities in the shared security responsibility model. Following major changes to the system, a penetration test must be carried out.

6. CONTACT POINTS

[DIGIT CLOUD CENTRE OF EXCELLENCE](#)

EC-SECURITY-INFOSEC@ec.europa.eu

(²⁹) In line with the cybersecurity strategy and the Cybersecurity Regulation, these should be stored in a central repository.

(³⁰) [SOC 2® - SOC for Service Organizations: Trust Services Criteria | AICPA & CIMA](#)
[BSI - C5 introduction](#)