Information Security Policy

Objective

The objective is to enhance information security at CEPI by ensuring Confidentiality, Integrity, and Availability through ISO/IEC 27001:2022 standard and our Information Security Management System (ISMS).

Contents

Objective 1
Contents 1
1 Definitions 2
2 Policy statement 3
3 Scope 3
4 Roles, Responsibilities & Communications 3
4.1 Roles and Responsibilities 3
4.2 Internal Communication 5
4.3 Communication with relevant Third Parties 5
5 Information Security Management System (ISMS) 5
5.1 Commitment to information security: 5
5.2 ISMS Objectives & Measures 5
5.3 ISMS & Regulatory Requirements 6
5.4 Information Security & Data Protection 6
6 Monitoring Controls 7
7 Document Management 7
8 Records Management 7
9 Policy Ownership, Compliance 7
9.1 Policy Exceptions 8
10 Document Control 8
10.1 Document Distribution 8

1 Definitions

Terminology	Definition
Availability	Characteristic of the information by which authorized persons can access it when it is needed.
Confidentiality	Characteristic of the information by which it is available only to authorized persons or systems. CEPI information classification is detailed in the Information Sensitivity Policy.
Data Protection	Process of safeguarding personal data, namely any information relating to an identified or identifiable natural person (as further defined in Art. 4(1) of EU Regulation No. 2016/679 (GDPR) against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
Employees	An individual with an employment contract directly with one of CEPI's three legal entities in Norway, United Kingdom, or the USA.
Associate	A CEPI associate is any non-employee engaged to provide services to CEPI or chosen or appointed to act or speak on behalf of CEPI. This includes, but is not limited to: paid consultants, temporary workers and individuals engaged through a professional employer organisation or other intermediary; external reviewers or other experts engaged by CEPI (paid or unpaid); interns and fellows (paid or unpaid) and members of CEPI's Board of Directors and advisory bodies (e.g., Scientific Advisory Committee, Joint Coordination Group).
Holistic Security Governance Committee	A committee constituted by CEPI top management having the competencies and powers set forth
Information Security	Set of technical, organizational, legal, and human measures necessary to prevent, detect and/or correct un-authorized use, misuse, modification, or failure of the information system.
Information Security Management System (ISMS)	Part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving information security and data protection.
Information Systems Security	Preservation of Confidentiality, Integrity, and Availability of information.
Integrity	Characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.
ISO 27001	An international standard about Security techniques — Information security management systems.
ISO 27005	An international standard about Information security, cybersecurity, and privacy protection – Guidance on managing information security risks.
ISO 27017	An international standard about Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO 27018	An international standard about Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
ISO 27701	An international standard about Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.
Privacy	The right and ability of any individuals to control, access, and determine (to disclose information or not) how their own personal information is collected, used, stored, and shared by others.
Third Parties	A third party is any person or business connected to your operations but not part of your organization's management.

2 Policy statement

The purpose of the Information Security Policy at CEPI (Coalition for Epidemic Preparedness Innovations), is to support the continuous efforts to ensure the Confidentiality, Integrity, and Availability of information belonging to our organization.

As an organization that values trust and credibility with our global partnership between public, private, philanthropic, and civil society organizations, we understand the importance of protecting against the evolving risks and threats to Information Security.

To achieve this purpose, CEPI has established and implemented a comprehensive Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022. This policy outlines our approach to managing Information Security, including our objectives and responsibilities, and reflects CEPI's commitment to ensuring the security of our data and that of its partners.

3 Scope

The scope of our Information Security Policy at CEPI covers all aspects of our organization's information assets, including those entrusted to our Employees, Consultants, Associates and Third-Party partnerships.

The Information Security Policy applies to all aspects of CEPI's information security practices and activities, encompassing the protection of sensitive information, data processing, storage, transmission, and disposal.

This policy is applicable to all Employees, Contractors, Associates, Third-party vendors, and other personnel who have access to our information assets. All employees, and associates shall comply with this policy and contribute to the ongoing improvement of our Information Security Management System (ISMS).

4 Roles, Responsibilities & Communications

4.1 Roles and Responsibilities

CEPI has identified and appointed competent employees under the following key information security roles and responsibilities:

Holistic Security Governance Committee:

- Leadership: Demonstrating commitment to the ISMS implementation and its continual improvement.
- Policy Establishment: Defining and approving the information security policy and objectives.
- Resource Allocation: Allocating necessary resources, including personnel, budget, and technology.

Information Security Officer:

- Managing and maintaining the ISMS implementation and compliance.

Risk Owner:

- Ensuring their information security risks are maintained at an appropriate level and mitigated when needed.

Human Resources:

- Ensuring controls as defined in the Statement of Applicability regarding personnel are applied and enforced.

Digital & Technology:

- Overviewing the implementation and maintenance of technical security controls, such as firewalls, encryption, and access controls and assisting in incident response and recovery efforts.

Senior Data Protection & Privacy Manager:

- Managing data breaches related incidents, ensuring compliance with data laws and regulations, and ensuring that third parties adhere to the organization's security policies and standards when handling sensitive data and providing services.

Legal and Compliance:

- Ensuring that the organization complies with relevant laws, regulations and standards, and reviews contracts and agreements to ensure they include necessary security clauses and align with organization's policies and standards.

Third-Party and Contractors:

- Ensuring that third parties adhere to the organization's security policies and standards when handling sensitive data and providing services.

Internal Audit Team:

- Developing Internal Audit Programme to be conducted at planned intervals of the ISMS to identify and report weaknesses or areas for improvement, to ensure adherence to ISO 27001 standards.

Employees and Associates:

- Adherence to security policies and procedures that are mandatory and applicable to roles and responsibilities, and ensure security incidents, breaches, or vulnerabilities are reported promptly.

Senior Security & Resilience Manager:

- Collaborating with the ISMS team to ensure that information security is integrated into the organization's business continuity plans.

4.2 Internal Communication

CEPI recognizes the importance of clear and effective communication among our Employees regarding Information Security. Therefore, all applicable Policies, and Procedures (SOPs) established, and implemented by CEPI, and stored on CEPI's Information Security Management System, shall be made available and communicated to all Employees and Associates, as appropriate to their respective roles and responsibilities.

The Human Resources Department is responsible for communicating the policies to all new hires. The Policy Owner must ensure that all employees and associates of CEPI, as well as appropriate contractors are familiar with this Policy and the requirement to report potential and actual breaches and system failures. As outlined in the Communication Plan, CEPI utilizes various channels based on the communication's purpose.

4.3 Communication with relevant Third Parties

CEPI must provide required information to enable all relevant Third Parties to:

- understand and assume their responsibilities and commitments in the operation of internal control related to security, Availability, Confidentiality, and privacy, including the system and its limitations (to allow users to understand their role within the system);
- report potential or actual breaches, systems failures, incidents, concerns, and other complaints; and
- understand changes on the above-mentioned topics in a timely manner on the matters of process, people, structure, or system changes.

The relationship owner communicates other relevant information to support the execution and operation of internal controls, when necessary, to the appropriate external vendor's team(s) through training and awareness initiatives.

Any public communication of the ISMS related information such as on the CEPI website, social media platforms or in the press must be approved before it is released and monitored.

5 Information Security Management System (ISMS)

5.1 Commitment to information security:

CEPI acknowledges that information is a critical business asset and the strategic importance of protecting CEPI and its information assets from all threats, whether internal, external, deliberate, or accidental.

5.2 ISMS Objectives & Measures

CEPI has identified the overall information security objectives:

- Ensure compliance with applicable laws, regulations, and guidelines.
- Meet the requirements for Confidentiality, Integrity and Accessibility for the organization's Employees, and Third Parties.
- Align Information Security measures to other CEPI policies on e.g., Organizational Policy Creation and Management Policy, and CEPI Cyber Risk Management Framework.
- Establish controls to protect the organization's information and information systems against theft, abuse and other forms of damage and loss.
- Motivate Associates and Employees to maintain responsibility for ownership and knowledge of information security, and to minimize the risk of security incidents.

- Ensure that Employees and Associates have adequate knowledge/training in line with their job responsibilities, to be reasonably educated about risks, remedies, responsibilities and reporting requirements.
- Ensure that the organization can continue its activities even if a severe security incident occurs.
- Ensure the protection of personal data (privacy).
- Ensure the Availability and reliability of services provided and operated by the organization.
- Ensure that external service providers operate in accordance with the organization's needs and requirements in terms of Information Security.

5.3 ISMS & Regulatory Requirements

This Information Security Policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to CEPI in the field of Information Security and Data Protection, as well as with contractual obligations.

CEPI must maintain a list of legal, regulatory, and contractual obligations.

Policies and procedures must be in place and provide required information to enable all relevant personnel to:

- understand and carry out their responsibilities and commitments for internal controls, including the system and its boundaries;
- report systems failures, potential or actual incidents, concerns, and other complaints; and
- understand the changes on the previous points in a timely manner (organisational, systems changes, etc.)

CEPI must communicate other relevant internal and external information to support the execution and operation of internal controls to key stakeholders through training, external certifications, and outreach initiatives (including security and privacy awareness programs to improve security and privacy knowledge).

5.4 Information Security & Data Protection

Data protection and privacy are critical facets of CEPI's ISMS and are underscored by CEPI's adherence to its regulatory and ethical obligations. This Policy must be read in conjunction with the Data Protection and Privacy Policy.

This commitment to data protection and privacy, as well as our legal, regulatory, and ethical obligations, are underpinned by the following principles:

- **Accountability:** all employees and partners must not only be informed but also compliant with CEPI policies and procedures. This compliance is crucial for maintaining the Integrity of internal controls, including understanding the scope and limitations of CEPI systems.
- **Reporting:** personnel must have clear guidelines on reporting system failures, potential or actual incidents, and concerns. This ability to respond is essential to address potential breaches in data security and privacy swiftly and effectively.
- **Awareness:** Employees and Associates must be kept abreast of any organisational or system changes promptly. This ensures that data protection and privacy standards are maintained even as the system evolves. Third parties must be properly informed of how their information is being processed, stored and protected, as well as of their rights and how to exercise them.

CEPI's management designs controls relevant to Security, Confidentiality, Integrity, Availability and Privacy, based on the Risk Management Policy.

These controls are described in detail in the CEPI ISMS Statement of Applicability document. When implementing controls, the ISO/IEC 27001:2022, Annex A, 27002, 27017, 27018, 27701 standards must be considered as guidance. Incompatible duties identified are to be segregated, and where such segregation is not practical, management must select and develop alternative control activities.

When designing or updating the controls, CEPI's management must determine the dependency and relationship between business processes, automated control activities, and technology based general controls relevant to Security, Availability, Confidentiality, Integrity, and Privacy.

CEPI's management, supported by appropriate teams, must develop policies and procedures that establish what is expected and relevant necessary to conduct controls related to Security, Availability, Confidentiality, Integrity, and Privacy.

6 Monitoring Controls

Ongoing monitoring is undertaken to evaluate the design and operational effectiveness of the ISMS and its controls to ensure Confidentiality, Integrity and Availability of data and systems. Continuous monitoring of security events must be maintained to ensure appropriate risk mitigation as well as compliance with applicable legislation.

Compliance with this Policy is monitored through the Internal Audit and Assurance group activities in accordance with the Annual Internal Audit and Assurance Plan, as agreed with CEPI Senior Management. Internal audits are performed at least on a yearly basis to ensure compliance with the ISO 27001:2022 standard as well as CEPI's policies and standards.

Identified non-conformities results of audits and assessments must be evaluated and communicated, where appropriate, to parties responsible for taking corrective action. CEPI' s Management ensures that correction and corrective actions are implemented in a timely manner.

CEPI expects Employees and Third Parties to report any suspicion of non-compliance immediately directly to the Policy Owner or, if appropriate, raise concerns in accordance with the CEPI Whistleblowing Policy.

7 Document Management

The current version of this document is effective as of the last update set out below. As the Policy owner, assisted by appropriate and competent teams, is responsible for the review, and updates, as appropriate, to policies and procedures at least annually to ensure their relevance to the processing and monitoring of control activities.

8 Records Management

Records shall be kept for a period enabling auditors to cover at least the period audited. Records related to a security or privacy incident shall be kept at least until the incident is closed and for an appropriate period beyond closure. In all cases, the retention of records shall comply with CEPI policies and applicable laws and regulations.

9 Policy Ownership, Compliance

The Chief Operating Officer is the owner of this Policy and are responsible for the implementation of its principles in CEPI's operations. It is the responsibility of the Policy Owner to ensure that appropriate level of information, awareness and training is provided to relevant Employees to ensure compliance with this Policy.

Non-compliance with this Policy and related policies may result in disciplinary action against those responsible under the disciplinary procedure detailed in CEPI's Employee Handbook.
This may include disciplinary action, up to and including termination of employment, and civil litigation and/or criminal prosecution to the full extent permitted by law.

Any breach of this Policy by a third party, may give rise to withdrawal of CEPI information technology resources to such third party, contract termination and/or civil litigation and/or criminal prosecution to the fullest extent permitted by law.

Individual compliance with any aspect of this policy may be monitored and reviewed by line manager. Any identified non-compliance with this Policy shall be notified to and reviewed by the Information Security Officer and Head of Compliance.

9.1 Policy Exceptions

Circumstances may arise where policy exceptions must be considered. In such circumstances, an exception can be granted momentarily or permanently to this policy by the COO. Exception requests to obtain exemption must follow the documented process. Exemptions are reviewed on an annual basis and must be re-approved by the COO.

IO Document Control

Title	**Information Security Policy**
Policy Owner	**Fernando Pons - COO**
Linked documents	Data Protection & Privacy Policy ISMS Master Document List ISMS Statement of Applicability document
Approved by	**Board EIC**
Data of approval	**May 2024**
Version Number	**2.0**
Review frequency	**Annually**
Next review date	**May 2025**

10.1 Document Distribution

All Employees and Associates in CEPI, Norway, UK, and USA.