1. Purpose and Scope

This document has been created to define and help communicate the common policies for information **confidentiality, integrity and availability** to be applied across the entire CK Life Sciences. The policies described in this document represent the basis from which all other information security policies, procedures, and standards are developed.

This Information Security Policy applies to all members of the CK Life Sciences including business entities across all countries (further referred to as the 'CK Life Sciences' or 'CKLS').

It applies to the creation, communication, storage, transmission and destruction of all different types of information within the CK Life Sciences. It applies to all forms of information, including but not limited to electronic copies, hardcopy, and verbal disclosures whether in person, over the telephone, or by other means.

2. Policy

2.1 Accountability

Each person within the CK Life Sciences has a responsibility to protect information.

- Information security accountability and responsibility must be clearly defined and acknowledged throughout the CK Life Sciences.
- All parties within the CK Life Sciences (employees, consultants, contractors and temporaries) are accountable for their access to and use of information, e.g., additions, modifications, copying and deletions.
- All accountable parties must act in a timely, coordinated manner to prevent or respond to breaches of, and threats to, the security of information and information systems (manual or computerized, or a combination of both).

2.2 Proportionality

Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of the information.

- Information security measures shall be appropriate to the value and sensitivity of the information, and the threats to which the information is vulnerable.
- Information security measures shall compensate for the risks inherent in the internal and external environment where information is stored, transmitted, processed, or used.

2.3 Need to Know

Access to corporate information shall be restricted with the effect that only those who have an evident business reason to access the information shall be granted access.

2.4 Organisational Roles and Responsibilities

Organisational roles and responsibilities shall be identified in order to create, communicate, implement and govern the policy.

In addition to the specific roles and responsibilities identified here, it is the responsibility of each business entity management to see that the policies contained within this document are implemented within their domains.

2.4.1 Head of Group IT Department

The Head of Group IT Department shall be responsible for:

1. Establishment and improvement of the information security culture across the CK Life Sciences.
2. Management of the development, deployment and maintenance of the CK Life Sciences information security policies.
3. Assurance of the status of information security across the CK Life Sciences, including the status of the proper deployment of and compliance to the CK Life Sciences' information security policies.
4. Coordination of activities related to significant security matters.

In particular, the Head of Group IT Department shall:

- Publish standards for compliance with this policy as necessary.
- Review the effectiveness of the CK Life Sciences' information security measures, including the reviewing and monitoring of security incidents within the CK Life Sciences if necessary.
- Implement reporting procedures for business entities on their information security status and significant information security matters.
- Own information security governance and risk appraisal approach at the CK Life Sciences level.
- Facilitate the understanding of potential threats, vulnerabilities, and control techniques across the CK Life Sciences.
- Monitor information security trends internal and external to the CK Life Sciences and keep the CK Life Sciences senior management informed about information security- related issues and activities affecting the organization.

2.4.2 Information Security Custodian

The management of each business entity, shall appoint an Information Security Custodian for business entity. The Information Security Custodian shall be responsible for:

1. Establishment and improvement of the information security culture in a business entity.
2. Ensuring the development & deployment of additional business entity policies, procedures and standards to support the CK Life Sciences Information Security Policy and related policies, procedures and standards.

3. Assurance of the status of information security in a business entity, including the status of the proper deployment of and compliance with the business entity's and the CK Life Sciences' information security policies, procedures and standards.

4. Coordination of activities related to significant security matters.

In particular, the Information Security Custodian shall:

- Define additional information security roles and responsibilities within the business entity.
- Ensure the deployment of methodologies, processes and risk assessments in support of the CK Life Sciences information security policies, procedures & standards.
- Provide information security education, and ensure training sessions are conducted and attended.
- Assist business entity management to establish an effective response plan to handle information security incidents.
- Implement reporting procedures in the business entity on its information security status, and reporting to business entity management and the CK Life Sciences as necessary.
- Review the effectiveness of the business entity's information security measures, including the reviewing and monitoring of security incidents within the business entity and reporting to the CK Life Sciences if necessary.
- Help the business entity to consider information security risks in both ongoing and planned operations.
- Work with business entity management on information security risk appraisal.
- Facilitate the understanding of potential threats, vulnerabilities, and control techniques within the business entity.
- Monitor information security trends internal and external to the business entity and keep the business entity senior management informed about the information security-related issues and activities affecting the business entity.

2.4.3 Information Owner

The management of each business entity shall ensure that every piece of CK Life Sciences information is assigned an owner, referred to as "Information Owner". The term Information Owner in this document only applies to information security matters as related to this policy, and does not imply any form of legal ownership over the information.

In general, unless otherwise designated,

1. The creator of a piece of information shall be assumed to be the Information Owner.

2. For information received from external parties, the designated recipient shall be the default Information Owner.

The Information Owners are responsible to:

- Determine the authorisation and handling process associated with information.

- Take steps to ensure that appropriate controls are utilised in the storage, handling, distribution, and regular usage of information.

- Ensure that the information is available to all relevant personnel who need to know.

2.5 Information Management

2.5.1 Classification and Labelling

To manage and control access to information, business entity executives should consider formal classification and labelling of information, but having due regards to the needs of the business, cost (both internal and external) and practicality. Guidelines for formal classification are given in Appendix 1.

2.5.2 Consistent Protection

Information must be protected consistently, irrespective of where it resides, what form it takes, or what purpose it serves.

2.5.3 Information Disclosure

The management of each business entity, in consultation with the Information Security Custodian and in compliance with standards issued by the Head of Group IT Department, will establish and implement specific rules and guidelines for disclosure and receipt of any sensitive information, e.g., the issuance or signing of Non Disclosure Agreements, and handling of sensitive information received from external parties.

2.5.4 Change Control

Changes related to information security processes, including system and procedural changes, must be properly approved, documented, and communicated to appropriate parties. Formal change control procedures should be implemented for confidential information.

2.6 Access Control

Appropriate controls shall be established to balance access to information and supporting information resources against the associated risk.

- Access to information must be controlled on a need-to-know basis guided by specific business requirements commensurate with its classification disregarding the seniority of those who request for access

- Access to information is subject to authorisation. An authorisation process shall be implemented for every information system, computerised or not. The authorisation process shall be sanctioned by the Information Owner and the applicable Information Security Custodian

2.7 Assessment

The risks to information and information systems shall be periodically assessed.

- Business entity executives shall ensure that risk assessments are conducted regularly and whenever circumstances require, in order to determine the effectiveness of the controls installed to protect the information. Weaknesses identified through the risk assessment process shall be addressed within a time frame in line with the likelihood and impact of the risks.

- The information security implementation for each business entity shall be independently reviewed regularly or whenever significant modifications with the business entity would potentially change its risk environment.

2.8 Awareness

All parties, with a need to know should have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information.

- Appropriate qualifications related to integrity, need-to-know, and technical competence of all parties shall be verified before access to information or supporting information resources is provided.

- All CK Life Sciences personnel must understand the CK Life Sciences' policies and procedures on information security, and must agree to perform his work according to such policies and procedures.

- CK Life Sciences's business partners, suppliers, customers, and other business associates must be made aware of their information security responsibilities via specific language appearing in contracts which define their relationship with the CK Life Sciences.

- The Head of Group IT Department shall establish channels and organisation to share and communicate information security - related knowledge and experience - amongst CK Life Sciences business entities.

2.9 Education

This Information Security Policy shall be communicated to all personnel to ensure that they understand this policy and their responsibilities under it.

- Training on information security is mandatory for all employees. Training shall include policies, standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences of failure to comply. Training and refresher training shall be conducted regularly.

- All CK Life Sciences personnel must be provided with supporting reference materials to allow them to properly protect and otherwise manage CK Life Sciences information.

2.10 Incident Management

All information security incidents shall be responded to expeditiously and effectively to ensure that any business impact is minimised and that the likelihood of experiencing similar incidents is reduced.

- Information security incidents, i.e. anything that compromises or may potentially compromise information security, must be reported to appropriate parties, including the relevant Legal Department (CK Life Sciences Legal or business entity Legal, as applicable), the information owner, Information Security Custodian, and those who may be potentially affected by the incident within the business entity or in other entities within the CK Life Sciences. The steps taken to deal with the incidents and the resolution of the incidents must also be reported.

- Each business entity should have an effective information security incident response plan. The plan should describe, inter alia, (i) the composition and roles of the incident response personnel in the entity; (ii) communication with internal parties and external parties (the latter include customers, law enforcement agencies, regulators and the media); and (iii) the technological means, tools, and resources that will be used to identify the causes of the incident and to recover compromised data in a timely manner.

2.11 Operational Continuity and Contingency Planning

Information systems shall be designed and operated in such a way as to preserve the continuity of organisational operations.

- CK Life Sciences business entities shall have in place a plan to ensure that confidentiality, integrity, and availability of information is maintained to support business continuity when disruptions or disasters occur. The plan must be documented and communicated to relevant parties, and relevant drills performed regularly.

2.12 Legal, Regulatory, and Contractual Requirements

All legal, regulatory, and contractual requirements pertaining to information security (including applicable personal data protection and privacy laws) must be considered and addressed.

- When dealing with information security, the CK Life Sciences must, at a minimum, satisfy all applicable legal and regulatory requirements. It is the responsibility of every business entity to assure compliance with their respective regulatory and other legal requirements.

2.13 Information Privacy

Each business entity shall take due care in implementing information security measures to comply with applicable laws and information privacy and data protection policies of the business entity and the CK Life Sciences.

2.14 Documentation and Management of Policies

Policies and supporting standards, baselines, procedures, and guidelines shall be developed and maintained to address all aspects of information security. Such guidance must assign responsibility, the level of discretion, and the level of risk each individual or organisational entity is authorised to assume.

- This Information Security Policy is a living document and needs to be periodically reviewed and maintained. This maintenance and updating of this policy may include but is not limited to changes in regulatory concerns and laws, core businesses, and technology.

2.15 Exceptions to Policy

Exceptions to this policy may sometimes be required for business or practical purposes. This must be authorised by the person in charge of the business entity on the advice of the Information Security Custodian and after approval by the Head of Group IT Department.

- Exceptions, including their rationale, duration, and details, must be documented within a reasonable time frame.

- Exceptions shall be reassessed and re-approved when there are changes in business or risks, change of responsible executive, or after a period determined by the Head of Group IT Department, whichever comes first.

2.16 Violations of Policy

Violations of the Information Security Policy are considered to be serious infractions and will be dealt with appropriately, with an emphasis on prevention of future infractions.

- Non-compliance with information security policies, standards, or procedures is a ground for disciplinary action including termination of employment.

Appendix 1: Guidelines on Data Classification and Labelling

1. Data Classification

All information should be classified according to its level of sensitivity. Three default categories are suggested. They are:

- Public
- Internal Use
- Confidential

These classifications have been designed to protect information from unauthorised disclosure, use, modification or deletion, based on 'need to know' policy, i.e. access to corporate information shall be restricted with the effect that only those who have an evident business reason to access the information shall be granted access.

Information which is not specifically classified should be scrutinised to ascertain the classification, and if this cannot be done then the information should by default be deemed to be classified as Internal Use, and therefore should be treated accordingly.

In this appendix:

- An access control list for a piece of information is a list of persons or parties authorised to have the right to access the information.
- A distribution list is a list of persons or parties to which a piece of information is physically distributed.

1.1 Public

"Public" classification applies to information that has been explicitly approved by the management of the relevant business entity for disclosure to the public outside of the CK Life Sciences.

Only designated persons may classify information as Public.

Only designated persons may disclose Public information. Such disclosure shall follow predefined procedures, rules and guidelines.

1.2 Internal Use

"Internal Use" classification applies to information that, if disclosed inadvertently or without authorisation, could have negative consequences for the business unit, the sub-group or CK Life Sciences and may induce costs in redressing those consequences.

Internal Use information shall not be disclosed to anybody outside of the CK Life Sciences without prior approval by the Information Owner. If the Internal Use information has any access control list, it shall not be disclosed to any other persons outside such access restriction without prior approval by the Information Owner. Internal Use information without an access control list may be disclosed within the CK Life Sciences.

Information Owner may also impose additional disclosure or handling restrictions to Internal Use information. Additional restrictions must not weaken the basic disclosure rules stated in this document.

1.3 Confidential

"Confidential" classification applies to information that, if disclosed inadvertently or without authorisation, could have significant negative consequences for the business unit, the sub-group or CK Life Sciences and may induce significant costs in redressing those consequences.

Confidential information should always have a distribution list or access control list, and should not be disclosed to any persons outside such distribution list or access control list without prior approval by the Information Owner. In the absence of an access control list, the distribution list is deemed to be the access control list. In the absence of both the distribution and access control lists, Confidential information shall not be disclosed to anybody without prior approval by the Information Owner.

Information Owner may also impose additional disclosure or handling restrictions to Confidential information. Additional restrictions must not weaken the basic disclosure rules stated in this document.

In addition, Confidential information must be further protected against deliberate and inadvertent unauthorised disclosure in its handling, including display, storage, transmission and disposal.

Due to the diversity of CK Life Sciences business and local legislative, CK Life Sciences business units should further take into the account of their business needs, the compliance to various legislation and industry requirements to set up the desirable categories. However, the ultimate categories shall be able to be mapped into the 3 default categories and shall not violate or contradict to the principles set out in this policy.

2. Information Labelling

Management of business entities is responsible for assessing, designing and implementing applicable specific procedures for information labelling for their respective business entities. However, such activity should be justified and supported by the following criteria:

1. It is required by local legislation, or

2. Without other alternatives, individual labelling is the only way that stakeholders could aware of the sensitive of the information, and

   I it is technically feasible, and

   II it is economically feasible. That is, the total benefit of such exercise outweighs the cost including on-going maintenance cost.

If a business entity does decide to go ahead with labelling, the following rules should apply:

- Confidential information should be the first to be labelled.
- The Information Owner is responsible to label the information according to its classification.
- Only the Information Owner or a person designated by the Information Owner should be authorised to change the classification label on information.
- The classification label should be readily apparent.

- The access control list and any additional restrictions should be clearly stated on the classification label or otherwise be readily apparent. For example, a classification label may be “Internal Use – For Company X Use Only” or “Confidential – For Department XX Use Only” or “Internal Use – For CK Life Sciences Internal Use Only”.

- The access control list or additional restrictions cannot replace the classification, i.e. irrespective of any additional restrictions, the classification of the information (e.g. *Confidential*) should be on the label.