Hutchison Telecommunications Hong Kong Holdings Limited
和記電訊香港控股有限公司

(Incorporated in the Cayman Islands with limited liability)
(Stock Code: 215)

INFORMATION SECURITY POLICY

I. Policy Statement

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 Group (comprising Hutchison Telecommunications Hong Kong Holdings Limited ("**HTHKH**"), its subsidiaries and controlled affiliates). The policies described in this document represent the basis upon which all other information security policies, procedures, and standards are developed.

This Information Security Policy ("**Policy**") applies to all members of the Group including all business units.

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

Questions in relation to this Policy should be directed to the Head of IT Security & Compliance.

II. Principles

2.1 Accountability

Each person within the Group has a responsibility to protect information.

- Information security accountability and responsibility must be clearly defined and acknowledged throughout the Group.

- All parties within the Group (including employees, outsourcing managed services and outsourcing call centres and teleservice centres, 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 computerised, 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 should be appropriate to the value and sensitivity of the information, and the threats to which the information is vulnerable.

- Information security measures should 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 such 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 in this Policy, it is the responsibility of each business unit management to see that the policies contained within this document are implemented within their domains.

2.4.1. Head of IT Security & Compliance

The Head of IT Security & Compliance shall be responsible for:

1. Establishing and improving the information security culture across the Group.

2. Managing the development, deployment and maintenance of the information security policies of the Group.

3. Ensuring the status of information security across the Group, including the status of the proper deployment of and compliance with the information security policies of the Group.

4. Coordinating activities related to significant security matters.

In particular, the Head of IT Security & Compliance shall:

- Publish standards for compliance with this Policy as necessary.

- Review the effectiveness of the information security measures of the Group, including the reviewing and monitoring of security incidents within the Group if necessary.

- Implement reporting procedures for business units on their information security status and significant information security matters.

- Assume ownership of information security governance and risk appraisal approach at the Group level.

- Facilitate the understanding of potential threats, vulnerabilities, and control techniques across the Group.

- Monitor information security trends internal and external to the Group and keep the Group senior management informed of information security-related issues and activities affecting the organisation.

2.4.2. Information Security Custodian

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

1. Establishing and improving the information security culture in a business unit.

2. Ensuring the development and deployment of additional policies, procedures and standards to support this Policy and related policies, procedures and standards.

3. Ensuring the status of information security in a business unit, including the status of the proper deployment of and compliance with the business unit's and the information security policies, procedures and standards of the Group.

4. Coordinating activities related to significant security matters.

In particular, the Information Security Custodian shall:

- Define additional information security roles and responsibilities within the business unit.

- Ensure the deployment of methodologies, processes and risk assessments in support of the information security policies, procedures and standards of the Group.

- Provide information security education, and ensure training sessions are conducted and attended.

- Assist business unit management to establish an effective response plan to handle information security incidents.

- Implement reporting procedures in the business unit on its information security status, and reporting to business unit management and the Group as necessary.

- Review the effectiveness of the business unit's information security measures, including the reviewing and monitoring of security incidents within the business unit and reporting to the Group if necessary.

- Help the business unit to consider information security risks in both ongoing and planned operations.

- Work with business unit management on information security risk appraisal.

- Facilitate the understanding of potential threats, vulnerabilities, and control techniques within the business unit.

- Monitor information security trends internal and external to the business unit and keep the business unit senior management informed of the information security-related issues and activities affecting the business unit.

2.4.3. Information Owner

The management of each business unit shall ensure that every piece of Group 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.

An Information Owner is responsible for:

- Determining the authorisation and handling process associated with information.

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

- Ensuring that the information is available to all relevant personnel on a need-to-know basis.

2.5 Information Management

2.5.1. Classification and Labelling

To manage and control access to information, business unit executives should consider formal classification and labelling of information, but having due regard 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 unit, in consultation with the Information Security Custodian and in compliance with standards issued by the Head of IT Security & Compliance, 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 unit 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.

- Information security implementation for each business unit shall be independently reviewed on a regular basis or whenever significant modifications with the business unit 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 Group personnel must understand the policies and procedures in terms of the information security of the Group, and must agree to perform his work according to such policies and procedures.

- The business partners, suppliers, customers, and other business associates of the Group must be made aware of their information security responsibilities through specific language appearing in contracts which define their relationship with the Group.

- The Head of IT Security & Compliance shall establish channels and organisation to share and communicate information security-related knowledge and experience - amongst Group business units.

2.9 Education

This Policy shall be communicated to all personnel within the Group 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 at least annually.

- All Group personnel must be provided with supporting reference materials to allow them to properly protect and otherwise manage Group 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 Legal & Regulatory Affairs Department, the Information Owner, Information Security Custodian, and those who may be potentially affected by the incident within the business unit or in other entities within the Group. The steps taken to deal with the incidents and the resolution of the incidents must also be reported.

- Each business unit 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) the communication process 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.

Each business unit 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 Group must, at a minimum, satisfy all applicable regulatory requirements. It is the responsibility of every business unit to ensure compliance with their respective regulatory and other legal requirements.

2.13 Information Privacy

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

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 Policy is a living document and needs to be periodically reviewed and updated. This process may include, among others, 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 unit on the advice of the Information Security Custodian and after approval by the Head of IT Security & Compliance.

- Exceptions, including their rationale, duration, and details, must be documented in a timely manner.

- Exceptions shall undergo a formal approval procedure with a documented risk assessment result and endorsed risk acceptance decision (in a Risk Acceptance Form) as a supporting prerequisite. Please refer to the "Risk Assessment Guideline - Exceptions" for details.

- 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 IT Security & Compliance, whichever comes first.

2.16 Violations of Policy

Violations of this 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.

(December 2023)

Appendix 1: Guidelines on Data Classification and Labelling

1. Data Classification

All information should be classified according to its level of sensitivity. Five default categories are adopted in HTHKH. They are:

- Public
- Proprietary
- Confidential - Customer
- Confidential - Company
- Highly 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 such 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 such information should by default be deemed to be classified as Proprietary, 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 Group.

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 Proprietary

"Proprietary" classification applies to information that, if disclosed inadvertently or without authorisation, could have negative consequences for the business unit or the Group and may induce costs in redressing those consequences.

Proprietary information shall not be disclosed to anybody outside of the Group without prior approval by the Information Owner. If the Proprietary 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. Proprietary information without an access control list may be disclosed within the Group.

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

1.3 Confidential (including Confidential – Customer, Confidential – Company and Highly Confidential)

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

Confidential information should always maintain a distribution list or access control list, and should not be disclosed to any persons outside the 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 Group business and local needs, business units should further take into account their business needs, the compliance to various legislation and industry requirements to set up the desirable categories. However, the ultimate categories should be able to be mapped into the five default categories and should not violate or contradict to the principles set out in this Policy.

2. Information Labelling

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

1. It is required by local law, or

2. Without other alternatives, individual labelling is the only way that stakeholders could be alerted of the sensitivity 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 unit decides to go ahead with labelling, the following rules should apply:

- Confidential information should be the first to be labelled.

- The Information Owner is responsible for labelling 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.

- 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 “Proprietary - For Company X Use Only” or “Confidential - Company - For Department XX Use Only” or “Proprietary - For HTHKH Group Proprietary 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 - Company) should be on the label.