# CP ALL Public Company Limited

# Information Security Policy

## 1. Purpose

The Information Security Policy (the Policy) provides comprehensive guidance to CP ALL in managing data across the organization in a consistent and effective manner that enables its businesses to achieve their strategic goals.Additionally, the Policy aims to mitigate data security (confidentiality, integrity and availability) risks and ensure CP ALL is compliant with all legal and regulatory requirements.

The Policy defines mandatory and recommended controls around collecting, processing, and sharing data. It also details corporate responsibilities related to data protection, data quality, data sharing, and group-wide data governance. The Policy is supported by relevant standards, where appropriate.

Non-compliance with the Policy and supporting standards may impact the integrity of data governance in CP ALL, resulting in adverse audit findings, regulatory censure, fines, criminal liability, contractual disputes, customer consent violations, disclosure of competitive information, and disciplinary actions for employees.

## 2. Scope

The Policy applies to This policy applies to all employees, contractors, consultants, temporaries, vendors and others engaged in activities for the benefit of CP ALL, including persons affiliated with third parties who have access to CP ALL's Information Resources.

## 3. Audience

All employees and relevant third parties.

## 4. Acronyms

| Acronym | Expanded form |
|---|---|
| CSO | Cyber Security Officer |
| Ex-Com | Executive Committee |
| ORC | Operational and Risk Committee |
| CP ALL | CP ALL Plc. |

## 5. Definitions

| Term | Definition |
|---|---|
| Confidentiality | Information is disclosed to only the authorized parties. |
| Integrity | Information is reliable, and only altered by authorized parties. |
| Availability | Information is accessible to authorized parties when needed. |
| Authorized Users | Authorized users are used to collectively refer to all such persons. Authorized users must adhere to this policy as a condition of continued employment as outlined in the policy. |

## 6. Authority and Accountability

- **Controls**: All businesses must implement appropriate procedures, technical controls, and monitoring to comply with the requirements in the Policy and supporting standards. The Cyber Security Officer must monitor compliance.
- **Governance**: Cyber Security Officer, with support from the businesses, is responsible for managing the Policy and supporting standards. The Executive Committee (the Ex-Com) approves the Policy, including revisions.

- **Implementation**: After the Policy is approved, the Cyber Security Officer will outline key activities across CP ALL businesses to effectively integrate technology governance with businesses' investment plans and ongoing activities.

The supporting standards are effective after approval from CTO. To the extent the Policy and supporting standards require revisions to businesses' practices or processes, businesses will be deemed compliant with those aspects of the Policy and supporting standards if they adhere to a documented action plan that addresses implementation of the Policy and supporting standards in a timeframe agreed to with the Cyber Security Officer. Businesses will be assessed for compliance with the Policy and supporting standards on at least an annual basis.

## 7. Risk Methodology

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual applications and systems.

Risk assessment should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

The information security risk assessment should have a clearly defined scope in order to be effective and should include relationships with risk assessments in other areas, if appropriate. Please refer to Information Security Risk Management Standard

## 8. Organization of Information Security

### 8.1 Internal Organization

CP ALL shall establish a management framework to initiate and control the implementation and operation of information security within the organization.

#### 8.1.1 Management Commitment to Information Security

CP ALL Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

#### 8.1.2 Information Security Coordination

CP ALL's information security team shall provide guidance, direction and authority for information security activities. The team will conduct regular internal and external compliance assessments at all CP ALL Locations in order to ensure compliance with information security requirements.

#### 8.1.3 Information Security Roles and Responsibilities

All information security responsibilities must be defined and allocated

1) Information Security Management must

a) Ensure that Information Security goals are identified, meet the organizational requirements, and are integrated in relevant processes.

b) Provide clear direction and visible management support for security initiatives.

c) Provide the resources needed for Information Security.

d) Review the appropriated Information Security Policy on an annual basis.

2) Security responsibilities must be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

3) Management must implement a training and compliance program to ensure that anyone acting on or using an information resource understands his or her roles and responsibilities. Training must be delivered before access to information resources is granted.

4) Security roles and responsibilities for employees, contractors and third parties include the following:

a) Individuals must act in accordance with the organization's Information Security policies.

b) Individuals must act to protect assets from unauthorized access, disclosure, modification, destruction or interference.

c) Individuals must execute security processes or activities consistent with assigned roles and responsibilities.

d) Individuals must act transparently and accept responsibility for actions taken.

e) Individuals must know how to and take action to report real or possible security events or risks.

5) For third parties, security roles and responsibilities must be included in Statements of Work, Service Level Agreements and/or contracts.

6) Information protection must be included in job and function descriptions, annual goals and objectives, performance appraisal, personal scorecard and executive compensation.

### 8.1.4 Contact with Authorities

CP ALL shall have procedures in place that define when and whom to contact in a timely manner if laws have been broken or if a major incident has occurred that impacts customer obligations.

#### 8.1.5 Contact with Special Interest Groups

CP ALL shall have an appropriate contact with special interest groups or other specialist security forums and professional associations, which are required to be maintained to keep information technologists well informed of emerging security risks. Reviews of supplier and industry information security alerts and other advisories will also be maintained.

#### 8.1.6 Information security in project management

CP ALL's information security program is required to be reviewed independently at planned intervals or when significant changes to the security implementation occur. Results will be recorded and maintained.

#### 8.1.7 Independent Review of Information security

CP ALL's information security program is required to be reviewed independently at planned intervals (at least annually or when significant changes to the security implementation occur). Results will be recorded and maintained.

### 8.2 External Parties

CP ALL shall maintain the security of the organization's Information Resources and Computing Resources that are accessed, processed, communicated to, and/or managed by external parties. Please refer to Supplier Security Management standard

## 9. Human resource security

### 9.1 Prior Employment

CP ALL shall ensure that CP ALL employees and contractors understand their responsibilities including information security, and to reduce the risk of theft, fraud or misuse of facilities.

### 9.2 During Employment

CP ALL shall ensure that all employees are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support the organizational security policy in the course of their normal work, and to reduce the risk of human error.

### 9.3 Post Employment

CP ALL shall protect the organization's interests as part of the process of changing or terminating employment. Please refer to Human Resource Security Standard

## 10. Asset management

### 10.1 Responsibility for Assets

CP ALL shall identify organizational assets and define appropriate protection responsibilities. All key information assets are required to be clearly identified, inventoried, documented and maintained by the process and group responsible for the asset. Ownership of this inventory should be formally established. Please refer to Asset Management Standard.

### 10.2 Information Classification

CP ALL shall ensure that information receives an appropriate level of protection in accordance with its importance to the organization. Information must be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

### 10.3 Media Handling

CP ALL shall prevent unauthorized disclosure, modification, removal or destruction of assets and interruption to business activities. Please refer to Asset Management Standard.

## 11. Access control

### 11.1 Business requirement of access control

CP ALL shall limit access to information and information processing facilities. An access control policy must be established, documented and reviewed based on business and information security requirements. Please refer to Access Control Standard.

### 11.2 User access management

CP ALL shall ensure authorized user access and to prevent unauthorized access to systems and services. Formal procedures must be in place to control the allocation of access rights to Computing Resources and services. The procedures must cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to Computing Resources and services. Please refer to Access Control Standard.

### 11.3 User responsibilities

CP ALL shall prevent unauthorized user access, and compromise or theft of Information Resources and Computing Resources. CP ALL employees should be required to follow Access Control Standard and Password management standard.

### 11.4 System and application access control

CP ALL shall prevent unauthorized access to systems and applications. CP ALL employees access to information and application system functions should be restricted in accordance with Access Control Standard and Password management standard.

## 12. Cryptography

CP ALL shall protect the confidentiality, authenticity or integrity of information by cryptographic means.

### 12.1 Cryptographic controls

Encryption should be employed to protect all CP ALL confidential Information. The required levels of protection are set out in Data Governance – Data Protection Controls spreadsheet and Cryptography and Key Management Standard.

## 13. Physical and environment security

### 13.1 Secure areas

CP ALL shall prevent unauthorized physical access, damage and interference to the organization's premises and information. Security perimeters shall be used to protect areas that contain Information Resources and Computing Resources. Also required are anti-intrusion and held-open alarms on access points. Please refer to Physical and environment security standard.

### 13.2 Equipment

CP ALL shall prevent loss, damage, theft or compromise of assets and interruption to CP ALL's operations. All equipment that is essential to CP ALL IT operations (processing, communications, transmission, storage) must be adequately protected against local environmental threats. Please refer to Physical and environment security standard.

## 14. Operations security

### 14.1 Operational procedures and responsibilities

CP ALL shall ensure correct and secure operations of information processing facilities. Formal operating procedures must be designed, documented, implemented and maintained for the day-to-day operations of all Computing Resources that store, process or transmit CP ALL information. The documents must be published and made readily available to all CP ALL employees with IT operational responsibilities. Please refer to Operations Security Standard.

### 14.2 Protection from Malware

CP ALL shall ensure that information and information processing facilities are protected against malware. All systems commonly affected both workstations and servers, must have

implemented the approved centrally managed virus protection software. Users are not permitted to disable, suspend, bypass or alter the state of the anti-virus software to reduce its effectiveness. Please refer to Operations Security Standard.

**14.3 Backup**

CP ALL shall protect against loss of data. Backup copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy. The required levels of information backup are set out in Operations Security Standard.

**14.4 Logging and monitoring**

CP ALL shall record events and generate evidence. The requirement of information security event collection and logging, Log Monitoring, Audit Logging, Time Synchronization, Security Log Retention and Rotation and Protection of Log Information can be found in Log Monitoring Standard.

**14.5 Control of operational software**

CP ALL shall ensure that the integrity of operation systems. All software installations and upgrades on centrally managed systems should be conducted in accordance with CP ALL's Change management process. Please refer to Operations Security Standard.

**14.6 Technical vulnerability management**

CP ALL shall prevent exploitation of technical vulnerabilities. The required of Vulnerability and Baseline Configuration Assessment is set out in Vulnerability Management Standard and Penetration testing framework.

**14.7 Information systems audits considerations**

CP ALL shall minimize the impact of audit activities on operational systems. Access to information systems audit tools shall be protected to prevent any possible misuse or compromise. Please refer to Operations Security Standard.

## 15. Communication Security

### 15.1 Network Security management

CP ALL shall ensure the protection of information in networks and its supporting information processing facilities. The required levels of protection of information in networks are set out in Network Security Standard.

### 15.2 Information transfer

CP ALL shall maintain the security of information transferred within an organization and with any external entity. The required levels of information transfer are set out in Network Security Standard.

## 16. System acquisition, development and maintenance

### 16.1 Security requirements of information systems

CP ALL shall ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. The design of all systems and applications should be required to follow Secure Software Development Life Cycle Standard and Secure Coding Guideline

### 16.2 Security in development and support processes

CP ALL shall ensure that information security is designed and implemented within the development lifecycle of information systems. Rules for the development of software and systems should be established and applied to developments within CP ALL. Please refer to Secure Software Development Life Cycle Standard

### 16.3 Test data

CP ALL shall ensure that test data must be protected and controlled. Production data being used in test environments shall be sanitized (anonymized) to protect the confidentiality of

the data. More information can be found in Data Governance – Data Protection Controls spreadsheet.

## 17. Supplier relationships

### 17.1 Information security in supplier relationships

CP ALL shall ensure protection of organization's assets that is accessible by suppliers. Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented. All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. Please refer to Supplier Relationships Standard

### 17.2 Suppler service delivery management

CP ALL shall maintain an agreed level of information security and service delivery in line with supplier agreements. Formal contracts must exist with all third party service providers to CP ALL. These contracts must define the agreed upon service level and delivery agreements and must address the on-going monitoring of performance against these commitments. These contracts should only be entered into after the successful completion of appropriate due diligence. All third party contracts must specify that providers of services to CP ALL are to be bound by CP ALL's policies and standards. These contracts should include the right for CP ALL to conduct a regular audit of performance against committed service levels and for compliance with CP ALL requirements. Please refer to Supplier Relationships Standard

## 18. Information security incident management

### 18.1 Management of information security incidents and improvements

CP ALL shall ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. The required is set out in Information Security Incident Management Standard.

## 19. Information security aspects of business continuity management

### 19.1 Information security continuity

Information security continuity should be embedded in the organization's business continuity management systems.

#### 19.1.1 Planning Information Security continuity

CP ALL must determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

#### 19.1.2 Implementing information security continuity

CP ALL must establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

#### 19.1.3 Verify, review and evaluate information security continuity

CP ALL must verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

### 19.2 Redundancies

CP ALL shall ensure availability of information processing facilities.

#### 19.2.1 Verify, review and evaluate information security continuity

Information processing facilities must be implemented with redundancy sufficient to meet availability requirements.

## 20. Compliance

### 20.1 Compliance with legal and contractual requirements

CP ALL shall avoid breaches of any law, statutory, regulatory or contractual obligations related to information security and of any security requirements. Please refer to Compliance Standard

### 20.2 Information Security Reviews

CP ALL shall ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

## 21. Exceptions

Businesses must comply with the Policy and supporting standards. Business that cannot comply must obtain approval from the ORC for an exception. The appropriate business owner must provide evidence to the CSO periodically to demonstrate compliance of their businesses with the Policy and supporting standards. Business owners may approve reasonable exceptions for certain business and functions for defined periods of time.

The CSO may endorse exceptions for up to one year. Any exception required beyond one year must be endorsed by the ORC.

## 22. References

*Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013*

*Information technology - Security techniques - Code of practice for information security controls (second edition), ISO/IEC 27002:2013*