

Summary of CDL Information Security Policy

Public Disclosure

Version 3.1 | September 2026

Prepared as a public-facing summary of CDL's Group-wide Information Security Policy and related governance documents.

Summary for Public Disclosure

City Developments Limited ("CDL" or the "Group") recognises that information security is fundamental to its business operations, digital transformation and the trust of its shareholders, customers, employees and business partners.

CDL has established a Group-wide Information Security Policy (the "Policy") that sets out the Group's commitment to protecting its information and technology assets through appropriate organisational, people, physical and technological controls.

The Policy is modelled on and aligned with ISO/IEC 27001:2022 and ISO/IEC 27002:2022 and serves as the overarching framework for CDL's supporting information security standards, procedures and guidelines. These include the CDL Cyber Incident Response Plan, CDL Group IT Acceptable Use Policy, CDL Data Classification, Handling and Disposal Policy, CDL AI Governance and Security Framework and CDL Generative AI Usage Guide.

The Policy applies across the CDL Group to employees, contractors and relevant third parties, and covers IT systems under CDL's administrative responsibility, including systems hosted on-premises, in cloud environments, through Software-as-a-Service (SaaS) platforms or managed by third-party service providers.

The Policy is approved by CDL's Executive Management and reviewed annually, as well as when significant changes occur in the business, technology or regulatory environment. The current version, Version 3.1, was approved in September 2026.

1. Introduction

The Policy establishes the baseline information security requirements applicable across the CDL Group. Group entities and subsidiaries may adopt additional requirements where necessary to address their specific business, risk, legal or regulatory obligations.

Information security requirements apply throughout the lifecycle of CDL's information and technology assets, irrespective of whether systems are operated internally, hosted in the cloud or managed by third parties.

2. Information Security Objectives

CDL's information security programme is guided by four principal objectives:

- **Protect information and technology assets** - preserving their confidentiality, integrity and availability through a risk-based approach.
- **Maintain compliance** - with applicable legal, regulatory and contractual requirements.
- **Strengthen IT continuity and cyber resilience** - so that critical business services can withstand, respond to and recover from security incidents and disruptions.
- **Promote a strong security culture** - by ensuring that employees and relevant stakeholders understand and fulfil their information security responsibilities.

3. Information Security Policy Mandates

3.1 Organisational Controls

Governance, Roles and Risk Management

CDL establishes supporting standards, procedures and guidelines to implement the Policy and communicates relevant requirements to employees, contractors and third parties.

Information security responsibilities are defined across the organisation. Executive Management provides governance and oversight; IT Security establishes and monitors the Group's security programme and security posture; IT teams design, implement and operate technology in accordance with established requirements; users are responsible for the secure use of CDL systems and information; and third-party service providers are required to comply with applicable CDL security requirements.

Information security risks are managed within CDL's broader enterprise and IT risk management frameworks and are considered throughout the lifecycle of technology projects and services.

Information Classification and Asset Management

CDL classifies and protects information according to its sensitivity and business requirements. The CDL Data Classification, Handling and Disposal Policy establishes requirements for the secure handling, storage, transmission, retention and disposal of information throughout its lifecycle.

Ownership is assigned for IT assets, and inventories of systems, hardware and software are maintained and periodically reviewed. Technology lifecycle management processes are also established to address ageing or unsupported technologies before they create unacceptable security or operational risks.

Identity, Authentication and Access Control

Access to CDL information and systems is managed according to business need, least-privilege and segregation-of-duties principles.

Individual user identities, strong authentication controls and additional safeguards for higher-risk access are implemented where appropriate. Privileged access to critical systems is subject to enhanced approval, protection and monitoring.

User access is periodically reviewed and revoked when it is no longer required. Third-party access is similarly controlled, limited to defined business purposes and subject to appropriate approval and review.

Supply Chain and Third-Party Security

CDL manages information security risks arising from suppliers and third-party service providers throughout the relationship lifecycle.

Security requirements are incorporated into relevant contractual arrangements, including requirements relating to protection of information, service continuity, incident notification and remediation of identified security weaknesses.

Security due diligence is performed for relevant service providers, particularly those that host CDL systems, process CDL information or support critical services. Where appropriate, independent security certifications or assurance reports may form part of the assessment.

CDL also considers security risks associated with software supply chains, including third-party and open-source software components.

Cloud and Artificial Intelligence Security

Cloud and SaaS solutions are subject to security risk assessment before adoption and are required to meet CDL's security requirements for areas such as identity, data protection, workload security, configuration management and monitoring.

CDL has also established an AI Governance and Security Framework governing the responsible and secure adoption of Artificial Intelligence. The framework addresses areas including governance, information security, data protection and privacy, safeguards for AI solutions, management of unauthorised AI usage and ongoing oversight of approved AI technologies.

Generative AI solutions intended for business use are subject to appropriate security assessment and security-by-design requirements. Users are required to use approved AI platforms and comply with CDL's Generative AI Usage Guide when handling CDL information.

Cyber Incident Response and IT Continuity

CDL maintains an established Cyber Incident Response Plan for the identification, assessment, escalation, containment, recovery and review of cybersecurity incidents. Employees and other relevant users are required to promptly report suspected information security incidents through established channels.

CDL also maintains an IT continuity and disaster recovery framework covering critical systems and their dependencies. Recovery requirements are established according to business needs, critical information is appropriately backed up, and recovery capabilities are periodically tested.

Business continuity and disaster recovery arrangements are reviewed and tested regularly, with relevant continuity requirements extended to critical third-party service providers where appropriate.

Legal Compliance, Personal Data and Intellectual Property

CDL requires compliance with applicable cybersecurity, privacy, legal, regulatory and contractual obligations and monitors material changes in the regulatory environment.

Personal data is protected in accordance with the Singapore Personal Data Protection Act 2012 ("PDPA"), other applicable privacy requirements and CDL's internal data protection policies.

Confidential information, intellectual property and proprietary information are subject to appropriate safeguards. Employees and other users are required to use only authorised platforms and services when processing sensitive CDL information.

3.2 People Controls

Personnel Security and Security Awareness

Information security responsibilities form part of the employee lifecycle. Appropriate background verification is conducted for designated IT personnel and positions involving privileged access, and access and responsibilities are reviewed when individuals change roles or leave the organisation.

Users are required to use CDL systems responsibly and for authorised purposes and to understand their responsibilities for protecting CDL information.

Information security awareness training is provided to users with access to CDL systems, with organisation-wide cybersecurity awareness activities conducted regularly. Personnel performing specialised technical or security functions receive additional training appropriate to their responsibilities.

Users are also required to comply with the CDL Group IT Acceptable Use Policy.

3.3 Physical Controls

Physical and Environmental Security

CDL applies physical and environmental safeguards to information processing facilities such as data centres and server rooms to protect them against unauthorised access, damage and environmental threats.

Appropriate supporting infrastructure, physical access controls and monitoring are maintained according to the criticality of the facility. Relevant physical and environmental security considerations are also incorporated into the assessment of third-party hosting and cloud service providers.

IT equipment and storage media are securely sanitised or disposed of in accordance with established procedures to prevent unauthorised recovery of CDL information.

3.4 Technology Controls

Secure Architecture, Systems and Development

CDL applies security-by-design principles to the development, acquisition and implementation of technology solutions. Security architecture is based on principles including defence-in-depth, zero trust and least privilege.

Security risks are considered during solution design and when significant changes are introduced. Appropriate architectural and security reviews are conducted for relevant systems and projects.

Technology solutions are subject to secure development and change-management practices, including separation of development, testing and production environments; secure configuration and hardening; security assessment; and appropriate testing before deployment.

Internally developed applications follow established secure coding practices, supported where appropriate by recognised industry guidance such as the OWASP framework. Security testing and appropriate assessment of third-party and open-source software components form part of the development lifecycle.

Network, Endpoint, Data and Cryptographic Security

CDL implements layered security controls across its networks, endpoints, cloud environments, email services and information assets.

Network environments are appropriately segregated and protected against unauthorised or malicious activity. Remote access and third-party connectivity are subject to appropriate authentication and security controls.

Endpoints are protected using approved security technologies and secure configuration standards, with administrative privileges restricted according to business need. Personal devices permitted for business use are subject to applicable CDL security and device-management requirements.

Information is protected throughout its lifecycle, including while stored, transmitted or processed. Appropriate cryptographic controls are applied based on information sensitivity and risk, using recognised industry standards and secure management of cryptographic keys.

Security Operations, Vulnerability Management, Logging and Monitoring

CDL maintains processes for secure technology operations, including controlled production changes, configuration management, backup and recovery, vulnerability management, security logging and monitoring.

Security vulnerabilities are identified through a combination of technical assessment, security testing and threat intelligence and are prioritised for remediation according to risk, severity and exploitability.

CDL periodically assesses the effectiveness of its security controls through activities that may include independent audits, vulnerability assessments, penetration testing, cybersecurity exercises and other assurance activities.

Security-relevant events are centrally collected and monitored to support timely detection and response to suspicious or potentially malicious activity. Logging and monitoring controls are protected against unauthorised modification and are subject to appropriate oversight.

4. Enforcement and Compliance

Compliance with the Information Security Policy is mandatory for employees, contractors and relevant third-party users of CDL information and technology resources.

Failure to comply with applicable requirements may result in suspension or withdrawal of access privileges, disciplinary action, contractual remedies or other actions consistent with applicable laws and agreements.

CDL periodically reviews compliance with its information security requirements and may engage qualified independent parties to assess the design and effectiveness of its information security management practices.

Where full compliance with a security requirement cannot immediately be achieved, CDL maintains a formal exception process requiring appropriate justification, risk assessment, approval and compensating controls. Approved exceptions are time-limited and subject to periodic review.

A. Supporting Material – CDL Generative AI Usage Guide

The CDL Generative AI Usage Guide sets out the key requirements for responsible use of Generative AI including :

- use only CDL-approved AI platforms, applications, accounts and plug-ins;
- protect personal, confidential, restricted and other sensitive information;
- use appropriate prompts and verify AI-generated information before use or sharing;
- maintain appropriate human oversight and remain accountable for AI-assisted content and outcomes;
- use autonomous AI capabilities only within approved scenarios and defined boundaries, with significant decisions subject to authorised human review and approval; and
- respect intellectual property rights and protect CDL source code and proprietary information.

B. Supporting Material – Cyber Incident Response Plan

CDL maintains a Cyber Incident Response Plan to provide a structured approach to managing cybersecurity incidents :

- defines governance, roles, responsibilities and escalation requirements;
- covers detection, analysis, containment, eradication, recovery and post-incident review;
- provides for coordination with relevant business, corporate and external cybersecurity specialists;
- addresses applicable regulatory and stakeholder notification requirements; and
- is regularly reviewed and tested through simulations and cybersecurity exercises.

Material incidents are reviewed to identify lessons learned and strengthen preventive, detective and corrective controls.

Document basis. This summary is based on the CDL Information Security Policy (Version 3.1, September 2026) and the CDL Cyber Incident Response Plan (Version 1.5, November 2025).

Last updated: September 2026