# CodeGen International (Pvt) Ltd

Information Security Management System Policy

| | |
|---|---|
| **Document Number** | **:** PLCY-CG-ISMS-001 |
| **Classification** | **:** Internal |
| **Owner** | **:** Chief Information Security Officer (CISO) |
| **Effective Date** | **:** 01/07/2021 |
| **Last Review Date** | : 01/09/2022 |

**Document History:**

| Release Date | Version No | Author(s) | Description | Reviewed & Approved By |
|---|---|---|---|---|
| 30/06/2021 | 1.0 | CISO/ISM | Initial release of the document. | BoD |
| 01/09/2022 | 2.0 | Assistant Manager – Information Security | Updated Key Roles & Responsibility | ISSC |

## Contents

## 1. Purpose

The purpose of this Policy is to define information security, and to describe management's commitment to safeguard information at CodeGen International (Pvt) Ltd (hereafter referred to as "CodeGen") and the obligation of the employees, contractors and third parties to perform such purpose.

## 2. Policy Document Management

Information Security Management System Manual and Information Security Management System Procedure in combination will make the Information Security Management System Policy. Information Security Management System Policy is issued in accordance with the ***Mandatory ISMS Procedures (PR-CG-ISMS-011).***

### 2.1. Distribution

This is an internal document and should only be shared with employees at CodeGen and intended parties determined by the Chief Information Security Officer (CISO).

### 2.2. Enforcement

All employees, stakeholders and third party vendors having access to information and information systems of CodeGen shall comply with the CodeGen Information Security Policies. Such personnel should be required to execute an agreement with CodeGen, agreeing to abide by the Policy.

### 2.3. Exceptions

Approval for exceptions or deviations from the policies, wherever warranted, will be provided only after an appropriate assessment of the risks arising out of providing the exception. This assessment will be conducted by the Information Security Steering Committee (ISSC).

Exceptions will be agreed on a case-by-case basis, upon an official request made by the information asset/process owner or the user. These may arise, for example, because of local circumstances, conditions, practical limitations or legal reasons existing at any point of time. All exceptions must be submitted to the ISSC.

Approval for the exception will be provided by ISSC. The CISO will review all exceptions, as the case by case, bi-annually for validity and continuity.

### 2.4. Non-adherence and Disciplinary Action

All violations and attempted violations of the CodeGen Information Security Management System Policy by the employees of CodeGen shall result in disciplinary action instituted by the Human Resources (HR) Division in consultation with the Information Security Steering

Committee (ISSC) wherever appropriate. Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation as per the laid down HR disciplinary procedures.
All violations and attempted violations of the Information Security Policies by third party service providers shall result in appropriate action being instituted as per the terms and conditions of the agreements entered into with such service providers.

All violations of the Information Security Policies must be reported to the CISO.

### 2.5. Version History Control

It is the responsibility of ISMS Policy owners to ensure that additions and amendments are inserted into the ISMS Policy whenever change occurs and the copies of superseded policies, procedures or documents are discarded.
Master copies of superseded documents are secured by the CISO as an archive for future reference.

The numbering system will be as per the ***Mandatory ISMS Procedures (PR-CG-ISMS-011)***.

### 2.6. ISMS Manual Review

The ISMS Manual and all the policies will be reviewed once a year or as per the requirement arises in the organizational structure or roles and responsibilities of the ISMS are affected. Review shall incorporate changes in business objectives or the risk environment.

The review document will follow the document change management process as outlined in the ***Mandatory ISMS Procedures (PR-CG-ISMS-011).***

## 3. Scope

Scope of ISMS Policy shall be as per the latest version of ***ISMS Scope Document (MN-CG-ISMS-002)***.

## 4. Definitions

| | |
|---|---|
| Anti-Virus or Anti-Spyware Software | Software used to detect and prevent malicious or unauthorized program code such as viruses from being transmitted over the network or affecting computer systems. |
| Availability | Availability is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. Assets include things like information, systems, facilities, networks, and computers. All of these assets must be |

| | |
|---|---|
| | available to authorized entities when they need to access or use them. |
| Confidentiality | Confidentiality is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes. |
| Information Asset | Information assets are a definite piece of information, stored in any manner which is recognized as 'valuable' to the organization. |
| Information Asset Owner | The information asset owner has the responsibility of classifying the asset based on the CodeGen asset classification scheme and related guidelines (Refer CodeGen Information Asset Management Procedure and CodeGen ISMS Risk Assessment Procedure).<br><br>The owner of the information asset shall identify/approve the controls to be implemented to provide appropriate protection to the asset. In addition, the asset owner should annually review the access control policies and classification processes. The owner of the information asset is accountable for the security of the information asset. |
| Information Security | Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. |
| Information Security Event | An information security event indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an information security policy may have been violated or a safeguard may have failed. |
| Information Security Incident | An information security incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of your information and weaken or impair your business operations. |
| Information Security | Information Security Management System (ISMS) refers to a set of policies and processes established by management to assess the security requirements, develop and implement controls, evaluate |

| | |
|---|---|
| Management System (ISMS) | effectiveness of controls and implement improvements following a Plan-Do-Check-Act continuous improvement process. |
| Information Security Management System Auditor (ISMSA) | The Information Security Management System Auditor (ISMSA) performs periodic audits of CodeGen Information Security Management System and related processes. |
| Integrity | To preserve the integrity of information means to protect the accuracy and completeness of information. |
| Malicious Code | Malicious code includes all and any programs (including macros and scripts) which are deliberately coded in order to cause an unexpected (and usually, unwanted) event on an IT system. |
| Vulnerability | Vulnerability is a weakness in an information asset or group of information assets. An information asset's weakness could allow it to be exploited and harmed by one or more threats. |
| Security features of network services | Security features of network services could be:<br>Technology applied for security of network services, such as authentication, encryption and network connection controls;<br>Technical parameters required for secured connection with the network services in accordance with the security and network connection rules; and<br>Procedures for the network service usage to restrict access to network services or applications |
| Media | Storage media which contains CodeGen information. This includes hardware capable of storing CodeGen information (Compact Discs, USB storages, magnetic disks) |
| Service Level Agreements (SLA) | A contract between two parties that specifies, usually in measurable terms, what services will be furnished. |
| Change Management | Procedure of controlling changes to the infrastructure, application or any aspect of services in a controlled manner enabling approved changes with minimum disruptions. |

| | |
|---|---|
| Information Security Incident Management | Processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents. |
| Risk Assessment | Overall process of risk identification, risk analysis, and risk evaluation. |
| Information Security Manager (ISM) | Person who is responsible for managing the information security team and identifying information security risk and information security requirements of the organization. |
| Chief Information Security Officer (CISO) | Senior management person who is responsible for overall information security of the organization. |

Further, the terms and definitions given in ISO/IEC 27000 apply.

## 5. Information Security Policies

### 5.1. Management Direction for Information Security

**Our Vision**

"To be known globally for first mover end-to-end ICT Solutions."

**Our Mission**

"Crafting high quality, intelligent ICT solutions by a community of dynamic professionals through continuous research and knowledge sharing to optimize business processes of corporate enterprises."

**CodeGen IT Departments Information Security objective**

Increase stakeholder value by providing assurance on confidentiality, integrity and continuous availability of information and information assets.

CodeGen will achieve the information security objectives by:

- Working as a team;
- Approaching with commitment;
- Following work ethics;
- Ensuring compliance; and
- Establishing best practices.

**Information Security at CodeGen**

Information is a key asset of CodeGen and needs to be protected. Information can be stored in the form of written, printed, electronic media or with people. With the increase in interconnectivity, information is exposed to a growing number of threats and vulnerabilities. Information Security is the protection of information from threats and vulnerabilities to prevent unauthorized disclosure of information and preserve confidentiality, maintain integrity, and ensure business continuity, and minimize business risk to maximize return on investment.

We at CodeGen is committed to protecting the information and information processing assets or facilities of all our stakeholders, providing information security awareness to team members and to ensure continual improvement in information security in all our IT activities/processes while meeting applicable business, legal or regulatory and customer requirements through regular review of our Information Security Management System.

**Information Security Policy Statement**

CodeGen provides services for CodeGen business units and support in enhancing the business process while preserving the security of the information assets and customer information.

Within the context of this policy, the term "Security" in relation to information shall mean the safeguard of Confidentiality, Integrity and Availability properties of the information and information assets, as per the following definitions:

- **Confidentiality -** Information should not be made available or disclosed to unauthorized entities (i.e. persons, organizations, and systems);
- **Integrity -** Reliability of information will be maintained through protection from unauthorized, unintended modifications during transmission, storage, and retrieval; and
- **Availability -** Authorized users are granted timely and uninterrupted access to information. Availability will be based on the business requirement of the user.

To preserve the information security requirements, ensure compliance to contractual obligations and provide better and secure service to CodeGen business units and customers, CodeGen is committed to improve the efficiency of IT infrastructure and assure the security of its information assets at all times through an effective implementation and operation of an ISMS. Therefore, this information security policy of CodeGen dictates great responsibility to all stakeholders to protect information assets of CodeGen.

**CodeGen shall strive to secure information, safeguard information/ IT assets and develop efficient information systems by maintaining an effective information security posture at**

**CodeGen while being compliant to applicable legal, regulatory and contractual requirements.**

To meet the information security objectives of the organization, CodeGen shall establish, operate and maintain ISMS aligned with the requirements of the ISO/IEC 27001:2013 standard and leading practice guidelines. A risk management framework shall also be defined to analyze, assess and treat information security risk. The ISMS shall be implemented through a set of policies, procedures and standards, mandated by ISSC and communicated to all employees, temporary staff and third party contractors.

#### 5.1.1 Policies of Information Security

The set of CodeGen information security policies relevant to operate the ISMS and achieve the above policy statement is set out on this policy.

#### 5.1.2 Review of the Policies for Information Security

This policy will be approved by the Board of Directors on an annual basis. This policy will be reviewed by ISM and/or CISO and updated at least once a year to incorporate any additions, modifications, deletions to policies and controls that may be required due to changes, including but not limited to technology, regulations and contractual requirements. However non routine reviews shall occur if any significant change arises in the CodeGen's technical or business environment. Information security policy changes should be approved by the ISSC.

## 6. Organization of Information Security

**Purpose**

The purpose of this policy is to define a suitable information security organization structure, roles and responsibilities for coordination of information security activities across the organization.

**Responsibility**

The key process leads of CodeGen represents ISSC will be responsible for implementing this policy by identifying adequate resources and assigning specific security roles to individuals with proper competency and training.

### 6.1. Internal Organization

#### 6.1.1. Information Security Roles and Responsibilities

- CodeGen shall establish ISSC which is responsible for information security initiatives at CodeGen. ISSC shall be responsible for:

- Support the organization's information security goals, principles and initiatives through clear direction, demonstrated continuous commitment, and the explicit assignment and acknowledgement of information security responsibilities.
- Establish the ISMS policy, roles and responsibilities and ensure that the ISMS objectives and plans are established.
- ISSC shall establish, support and adequately resource the organization of information security within CodeGen.
- Provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS.
- Communicate the importance of achieving information security objectives and conforming to the information security policies within the organization, its responsibilities under the law and the need for continual improvement.
- Conduct Management Reviews of the ISMS Monthly.

- The standing members of the ISSC shall be constituted by the following officers at CodeGen.

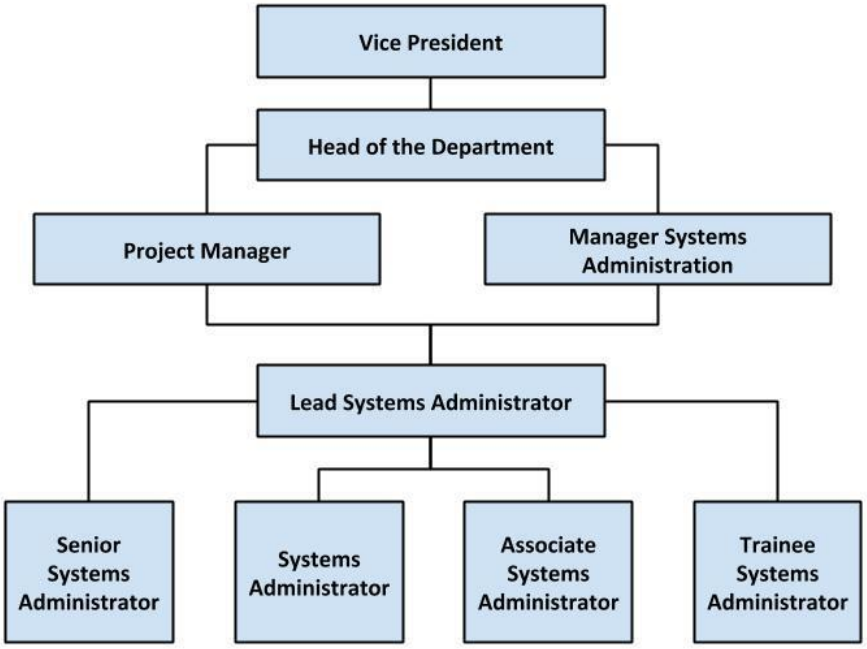
1. VP – Research and Development (Yohan Welikala)
2. Head Research and Development (Upali Kohomban)
3. CISO / Director – Delivery (Mohamed Shirazi)
4. Software Architect (Mafaz Hassan)
5. Senior Manager - Business Operations (Pahan Mapalagama)
6. Manager HR (Shenika Herath)
7. Project Manager (Gihan Jayawardena)
8. Assistant Manager – System Administration (Andrew Ferdinandus)
9. Admin & Finance Manager (Surendra Perera)
10. Assistant Manager – Information Security (Mahdi Shareef)
11. Manager - Legal (Dinusha Mohanasunderam)
12. QA Lead (Ashani Halpita)

The following may be permitted to attend the meetings of the ISSC by invitation:

- Representative from Legal division
- ISMS Auditor
- ISMS Consultants
- External Auditors
- Process Owners

- The roles and responsibilities of ISSC, the individual roles representing the ISSC and other roles supporting the ISMS are documented in the ***Information Security Roles and Responsibilities (PR-CG-ISMS-014)***.
- All information security responsibilities with regard to the protection of CodeGen sensitive information, IT systems and information processing facilities shall be clearly defined by ISSC through roles and responsibilities, work allocation and delegation of tasks. These will be communicated to the personnel using appropriate channels.
- ISSC will be assisted by CISO who shall coordinate the implementation and maintenance of information security controls.
- Security roles and responsibilities have been communicated to IT personnel and included in their respective job descriptions. These responsibilities include any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets or for the execution of particular security processes or activities.

## ITD Organizational Structure



### 6.1.2. Segregation of Duties

- All processes must adopt the principle of segregation of duties to the maximum extent possible. That shall constitute:
- Employees involved in operational functions must not be given additional responsibilities in CodeGen administration processes and vice versa.
- Employees shall not be able to approve functions performed by the superiors.
- In a situation where segregation of duties is not possible or practical, the process must include compensating controls; such as monitoring of activities, maintenance and review of audit trails, and management supervision.
- Monitoring processes shall be implemented to determine if any conflicting actions occur.

### 6.1.3. Contact with Authorities

- CISO, IT team members or relevant nominees from line management shall coordinate with appropriate authorities (e.g. law enforcement, fire department, municipal authorities).

### 6.1.4. Contact with Special Interest Groups

- Special interest groups or other specialist security forums and professional associations in order to improve knowledge of best practices, to be up to date with relevant security information and to provide suitable liaison points when dealing with information security incidents.

### 6.1.5. Information Security in Project Management

- Information security shall be addressed in project management, regardless of the type of the project.
- Information security shall be integrated into CodeGen's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes. The project management methods shall include:

a) Information security objectives in project objectives;

b) An information security risk assessment conducted at an early stage of the project to identify necessary risk treatment options.

c) Information security as part of all possible phases of the applied project methodology.

- Information security implications shall be addressed and reviewed regularly in all projects. Responsibilities for information security shall be defined and allocated to specific roles defined in the project management methods.

### 6.2. Mobile Devices and Teleworking

#### 6.2.1. Mobile Device Policy

- The usage of the mobile devices (i.e. laptops, mobile phones and mobile tablets) within the CodeGen network or connected to CodeGen network is subject to ***Acceptable Usage Policy***, which articulates the detailed ***Mobile Device Policy*** and the ***Bring Your Own Device (BYOD) policy***, hence all the users are expected to follow.
- Controls shall be established and appropriate security measures shall be adopted to protect against the risks of information compromised by using mobile computing and communication facilities.

#### 6.2.2. Teleworking

- Controls shall be established and appropriate security measures shall be adopted to protect against the risk of information compromised by teleworking. The scope of teleworking shall be defined as CodeGen employees connecting to back-end systems from out of premises through secure connectivity via VPN.
- In the event teleworking is required by contractors and vendors for an emergency, it shall be granted on a case by case basis which will be validated and approved by CISO. Such access and activities carried out during the access shall be monitored and logged.
- All teleworking users need to adhere to the ***Remote Access Policy*** mentioned in the ***CodeGen Acceptable Usage Policy***.

## 7. Human Resource Security Policy

**Purpose**

The purpose of this policy is to ensure that CodeGen employees, contractors and third party users understand their responsibilities, are suitable for the roles they are considered for, and to reduce the risk of human error, theft, fraud or misuse of facilities.

**Responsibility**

**HR Division:** shall be responsible for implementation of the controls and maintenance of all relevant records applicable to employees.

**IT Department:** shall be responsible for implementation of the controls and maintenance of all relevant records applicable to IT departmental contractors and third party service providers.

## 7.1. Prior to Employment

### 7.1.1. Screening

- Initial Background checks shall be carried out on all employees prior to the commencement of employment by CodeGen HR as per the HR procedures. A record of the reference checks shall be maintained in personal files. If necessary detailed checks of criminal records shall be performed for positions with access to extremely sensitive information.
- Background checks for third party vendors and/or suppliers shall be carried out by the respective Project Manager or Team Lead. These checks shall consider the past history of the vendors, background of the personnel who are involved in the project and references from their customers.

### 7.1.2. Terms and Conditions of Employment

- Confidentiality or non-disclosure agreements from all employees, contract employees, contractors, third party users reflecting the organization's need for the protection of information shall be obtained. Non-disclosure of information conditions are included in the standard employment contract with the relevant information security clauses.

## 7.2. During Employment

### 7.2.1. Management Responsibilities

- All the employees, contract employees, contractors and third party users are required to follow the information security policies and procedures. Respective division should train the staff on relevant policies and procedures.
- CodeGen management is responsible to ensure that all the employees, contract employees, contractors and third party users adhere to information security policies and procedures.

### 7.2.2. Information Security Awareness, Education and Training

- Appropriate awareness training and regular updates in organizational policies and procedures shall be provided to all employees of the organization as relevant to their job functions. Respective division should train the staff on relevant policies and procedures. Awareness training shall continue to be part of the induction training during the onboarding process.

### 7.2.3. Disciplinary Process

- A formal disciplinary process shall be initiated against employees violating laid down policies and procedures or committing security breach as per CodeGen's HR disciplinary procedure and HR division will conduct and record these in the Personal File in relevant stages.

### 7.3. Termination and Change of Employment

#### 7.3.1. Termination or Change of Employment Responsibilities

- HR division in conjunction with the concerned other departments shall follow the CodeGen employee termination process.
- In case of termination, a defined exit procedure shall be followed and a record of the same shall be maintained. Respective officer from the HR division ensures the return/review of all previously issued information and information processing assets.
- The access rights of all employees, contract employees and service providers to information and information processing facilities shall be removed upon termination of their employment / contract / agreement or modified for any change in their designation / status.
- Accordingly, employees will submit the Exit Clearance form to HR. The IT division is responsible for removing all access rights granted to exit employees.

## 8. Asset Management Policy

**Purpose**

The purpose of this policy is to define, implement and maintain appropriate levels of protection for CodeGen's information assets.

**Responsibility**

**Chief Information Security Officer (CISO):** Responsible for ensuring the implementation and adherence to the policy.

**Divisional Heads:** Responsible for ensuring that the controls are implemented as per the security classification levels.

**Information Asset Owners:** Asset owners are responsible for identifying major assets in each information system, identifying their security classification levels, ensuring appropriate labeling, handling and protection.

### 8.1. Responsibility for Assets.

#### 8.1.1. Inventory of Assets

- The identified Process Owners are responsible to prepare and maintain the information assets inventories at CodeGen. This should include all the IT assets including but not limited to systems, licenses, documents, physical assets and services, people, company image and reputation.

- The asset inventories shall be prepared, valued and maintained according to the guidelines provided within the ***Information Asset Management procedure (PR-CG-ISMS-002)*** and ***Risk Assessment and Treatment Procedure (PR-CG-ISMS-001).***

**8.1.2. Ownership of Assets.**

- All the information and assets associated with information processing facilities shall be assigned ownership to an individual with approved management responsibility.
- The asset owners shall be responsible for:
  - Ensuring that the information assets are appropriately classified;
    - Defining and reviewing on an annual basis, the access restrictions and classifications according to the ***Information Asset Management procedure (PR-CG-ISMS-002).***

**8.1.3. Acceptable Use of Assets**

- Rules/standards are defined for the acceptable use of information and assets associated with information processing facilities shall be implemented.
- All CodeGen's employees and any third party service providers who have access to CodeGen information or information systems shall follow the rules for the acceptable use of information and assets associated with information processing facilities. The rules and guidelines of acceptable usage are included in the ***Acceptable Usage Policy (PLCY-CG-ISMS-002).***

**8.1.4. Return of Assets**

- HR division in collaboration with the IT division or immediate supervisor/project team lead of the outgoing employee/service provider shall ensure that all assets of the organization e.g. ID cards, laptops are returned by the outgoing employee, service providers, contracted employees upon termination of their contract or at the end of employment.

**8.2. Information Classification**

**8.2.1. Classification of Information**

- Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization. The asset owners shall classify the assets as per appropriate security classification guidelines.
- Security classification level of the information asset shall be identified based on the impact that the asset will bring to the business if confidentiality, integrity or availability is breached.
- All information shall be classified to specify its level of sensitivity or confidentiality in order to protect sensitive information. The Information Asset Owner of the document or information owner must assign appropriate classification. Every piece of information

shall have an Information Asset Owner. The Information Asset Owner is the person holding the highest position in the relevant area. For e.g. all finance related information is owned by the Finance Division; all IT related information is owned by ITD, and all operations and IT departmental process information have the respective departmental heads as the highest owner.

- Where necessary, the Information Asset Owner shall specify a list of users that are allowed to access information of the asset, which lists names of people, designations, groups or roles or names of organizations that are authorized to view or modify the information.
- Classification of the information assets shall exist in all the documentation making it clearly visible.

#### 8.2.2. Labeling of Information

- Information assets shall carry an appropriate labeling to reflect its sensitivity and importance to CodeGen and handle the asset as per its sensitivity and importance.
- The labeling procedure is included in the ***Information Asset Management procedure (PR-CG-ISMS-002).***

#### 8.2.3. Handling of Assets

- Information handling procedure for each type of assets, physical and electronic format, and each type of activity is included in the ***Information Asset Management procedure (PR-CG-ISMS-002).***

### 8.3. Media Handling

#### 8.3.1. Management of Removable Media

- All removable media (e.g., CD / DVD writers, flash drives, etc.) and ports in computers without a business need to use such devices must be removed or disabled.
- Removable media must be stored in a safe and secure environment in accordance with the manufacturers' guidelines. Aspects such as temperature, humidity, magnetic fields, and physical access controls must be considered.
- Removable media with CodeGen's data must be handled only by authorized personnel. The process owner is responsible for ensuring that only authorized personnel handle the relevant removable media.
- Removable media must be reused and disposed only in accordance with the disposal guidelines provided in ***Information Asset Management procedure (PR-CG-ISMS-002).***

### 8.3.2. Disposal of Media

- When an information media becomes unusable or not required for business, it shall be disposed-off securely and safely. If proper care is not taken while disposing of the media, critical business information can be disclosed and misused. Procedures for disposal of media shall be followed to reduce the risk of corresponding security breach.
- All equipment containing storage media (e.g., fixed hard drives) must be checked to ensure that any critical business information assets and licensed software are removed, securely overwritten or destroyed prior to disposal. Following guidelines will be used to dispose or reuse storage media.

| Type of Equipment | Disposal | Reuse |
|---|---|---|
| Hard disks, floppy disks, tape, pen drives, chips, and other magnetic storage media. | ▪ Complete physical destruction of the disk. | ▪ Full reformat using a secure erasure program (use zero fill, pattern fill, etc.) with key deletion. |
| CD, DVD, Blu-Ray, and other optical storage media. | ▪ Physical destruction (i.e. breaking the disk). | ▪ No reuse. |
| Printouts and paper documents. | ▪ Shredding. | ▪ No reuse if confidential or sensitive information is contained. |

### 8.3.3. Physical Media Transfer

- Movement of media containing information shall be supported by a suitable authorization process.
- An inventory of media containing critical information (including backups) should be maintained and reviewed bi-annually by relevant process owners and they should raise a ticket in Jira to perform the backup.
- Movement of media shall be clearly logged to indicate when the movement is initiated, its source, destination and responsible officials for the movement.
- In case the confidential information needs to be printed on a common printer, the respective person who initiates the print is responsible for the information getting printed and ensuring that no printouts are left on the printer.
- While transporting information media to another location, care shall be taken to protect the media from damage, unauthorized modification.

## 9. Access Control Policy

**Purpose**

The purpose of this policy is to ensure that only authorized personnel are provided access to information and information processing facilities (including operating system, network and applications). Thus helps ensure protection of confidentiality, integrity and availability of information from unauthorized access, malicious intent, compromise and theft.

**Applicability:** The access control policy applies only to information processing facilities managed and administered by the CodeGen ITD.

**Responsibility**

**Chief Information Security Officer (CISO):** is responsible for monitoring implementation of this policy and responsible for approving access to information assets. Respective asset owners are responsible for reviewing access granted to their staff and third parties.

**System Owners:** are responsible for the implementation of this policy.

### 9.1. Business Requirements of Access Control

#### 9.1.1. Access Control Policy

- The creation, change and termination of user access rights and associated privileges shall be controlled and monitored. Processes shall be established to ensure that this is done in accordance with the Access Control policy.
- Users shall be assigned a unique ID before being allowed to access system components. In addition to assigning a unique ID, at least one of the following methods shall be used to authenticate users
  - Something you know, such as a password or passphrase;
  - Something you have, such as a token device or smart card; or
  - Something you are, such as a biometric.
- Access to the information systems will not be granted unless the authorization procedure has been completed.
- Explicit approval from authorized parties is required to use critical technologies/systems.
- Use of technology/system shall be authenticated with user ID and password or other authentication item.
- Access shall be restricted to least privileges necessary to perform job responsibilities.
- Access/privileges are assigned to individuals based on job classification and function on a need to know basis.

- Access rights of all users who have changed roles/jobs or have left the organization shall be revoked immediately.
- Users who are inactive for more than 180 days shall be dissabled. Last login date shall be considered to determine the inactive period.
- If the access is granted for a defined period (in case for vendors, temporary employees etc.), an automatic expiry date shall be configured at the access creation to ensure the access will be disabled at the time where the respective users duties are complete.

#### 9.1.2. Access to Networks and Network Services

- A formal authorization procedure shall be followed to allow access to networks and network services.
- Access to networked services such as servers, printers etc. shall be provided to users as per the access control policy. Additional controls such as secure Virtual Private Network (VPN) tunnels shall be used to access remote network services.
- CodeGen ITD shall ensure that its network will not be interconnected with any un-trusted voice or data networks, unless appropriately configured firewalls and other suitable protection measures are in place.
- ITD shall ensure that the access to the Internet is controlled via firewall.

### 9.2. User Access Management

#### 9.2.1. User Registration and De-Registration

- All CodeGen users having a need to use any of the company's information systems shall require an authorization from their respective Head in turn send it to ITD.
- The level of access granted to each user (including data center) shall be based on business requirement only.
- All users shall clearly understand the acceptable usage. An acknowledgement shall be obtained from the user stating that the user has read and understood the CodeGen acceptable usage policy, prior granting access to systems. No users will be given access to any system under any circumstances without this acknowledgement.
- A formal record of all employees registered to use the information systems shall be maintained by respective information system owners/ system administrators.
- The information systems shall be checked quarterly by the respective system owners to ensure redundant user IDs and accounts do not exist.
- The process owners will be responsible for the user account lifecycle management (including creations, deletions and modifications).

### 9.2.2. User Access Provisioning

- Systems owners shall provide access to their systems complying with this access control policy.

### 9.2.3. Management of Privileged Access Rights

- The privileges associated with each information system (e.g. for each operating system or application) and assigned individual users shall be identified.
- Privileges shall be allocated to individuals on a "need-to-use" or “need-to-know” basis.
- An authorization process shall be followed and a record of all privileges allocated shall be made. Privileges shall not be granted until the authorization process is complete.
- All activities related to privileged users shall be logged and monitored on a quarterly basis by ITD and reviewed by ISM to detect any misuse of privileges.

### 9.2.4. Management of Secret Authentication Information of Users

- All users shall be required to keep personal passwords confidential.
- All newly created user IDs shall be assigned a temporary password which shall be changed immediately upon first logon.
- Any user requesting a change in password shall be duly verified.
- The exchange of temporary passwords shall be carried out securely.
- Temporary passwords shall follow the password policy.
- Default vendor passwords shall be changed or disabled following the installation of the system or software.

### 9.2.5. Review of User Access Rights

- User access rights shall be reviewed at least once a quarter and after any change in the employment of the user such as promotion, demotion or termination. User access privilege management is carried out by raising Jira Tickets, the ITD and the IT Support team are responsible for handling them respectively.

CodeGen ITD is responsible for sending a report stating the username and rights given to the system for respective business units quarterly. In return, the business unit shall verify the rights and provide feedback to ITD for any actions to be carried out.

- Privileged user access rights (i.e. system administrators) shall be reviewed at least bi-annually by ISM.
- Necessary controls such as removal of extra access rights shall be conducted in case of any ambiguity found during the review.

#### 9.2.6. Removal or Adjustment of Access Rights

- Any modifications for existing user access rights will be approved by the relevant process owner and communicated to the relevant administrators for implementation.
- Removal of access rights shall be carried out as per 7.3.1. in this document.

### 9.3. User Responsibilities

#### 9.3.1. Use of Secret Authentication Information

- The job description for all positions shall be documented by the respective business unit. Security roles and responsibilities which are a part of the same job will be provided to CodeGen ITD. These responsibilities shall include any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets or for the execution of particular security processes or activities. Further user's responsibilities in the use of secret authentication information shall be communicated to users.

### 9.4. System and Application Access Control

#### 9.4.1. Information Access Restriction

- Access to application systems and information shall be restricted to authorized users only. The access restrictions shall be balanced in such a way that appropriate protection is provided for application and information while the business process continues smoothly. The access restrictions shall be in compliance with the business access control and operating access control policies.

#### 9.4.2. Secure Log on Procedures

- A general notice or warning shall be displayed, specifying that the computers and network devices shall be accessed only by authorized users.
- Only five (5) unsuccessful log-on attempts shall be allowed before the account is locked.
- The password, while being entered, shall be masked by symbols like the asterisk.
- No help messages shall be provided during the log-on procedure.

#### 9.4.3. Password Management System

- Procedures for enforcing and managing the user passwords shall be established and implemented to ensure user's identity and authenticity in accessing information resources. Following password policy shall be configured in the system.

**CodeGen Password Policy – User Level Password Policy**

- Following minimum password standards shall be used for all system level, domain level and application level user passwords. Password policy shall be implemented in all the systems/applications and infrastructure where possible. Any exceptions to the password

policy or if this cannot be technically enforced, such situations shall be documented, risk assessment and risk treatment shall be carried out accordingly.

| Password Setting | Configuration for information processing facilities where logical access required |
|---|---|
| Minimum number of characters | 8 characters |
| Enforcing password complexity | Enabled |
| Maximum password age | 60 days |
| Minimum password age | 1 days |
| Enforcing password history | 5 previous passwords |
| Account lockout threshold | 5 invalid logins |

**CodeGen Password Standard – Administrative Password Policy**

- Following minimum password standard shall be used for all system level, domain level and application level administrative passwords.

| Password Setting | Configuration for information processing facilities where logical access required |
|---|---|
| Minimum number of characters | 8 characters |
| Enforcing password complexity | Enabled |
| Maximum password age | 60 days |
| Minimum password age | 1 days |
| Enforcing password history | 5 previous passwords |
| Account lockout threshold | 5 invalid logins |

### 9.4.4. Use of Privileged Utility Programs

- Most operating systems have one or more system utility programs and commands that might be capable of overriding system and application controls. The use of such critical system utilities and Operating System (OS) commands shall be tightly controlled by not allowing privileged access of the OS to users who do not need it.

#### 9.4.5. Access Control to Program Source Code

- Adequate access control procedures shall be defined and established to authorize access to the program source codes.

## 10. Cryptography

**Purpose**

The purpose of this policy is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

**Responsibilities**

**Chief Information Security Officer (CISO):** shall be responsible for the implementation of this policy in consultation with the respective process owners/administrators.

### 10.1. Cryptographic Controls

#### 10.1.1. Policy on the Use of Cryptographic Controls

- Based on the business need, cryptographic controls shall be identified and implemented to provide appropriate level of protection to information and information systems.
- Adequate process or procedures on the use of cryptographic controls for protection of information shall be developed and implemented. When developing the procedures or process, consideration shall be given to:
  - Approach towards the use of cryptographic controls across the organisation;
  - Rules under which the business information is protected;
  - Required level of protection be identified after adequate risk assessment;
  - Required methods of protection of cryptographic keys and recovery methods in case of loss of or damage to those keys;
  - Roles and responsibilities of the personnel for implementation, management and generation of keys;

#### 10.1.2. Key Management

- All cryptographic keys shall be protected against modification, loss, destruction and unauthorized disclosure. A process or procedure shall be put in place for:
  - Generating keys for different systems and applications;
  - Generating and obtaining public key certificates;

- Distribution of keys to the intended users;
- Storing and archiving or back-up of the keys;
- Changing or updating the rules on keys when there is need;
- Handling on compromised keys while they are in transit or in storage;
- Recovery of damaged/corrupted or lost keys for recovery of encrypted business information; and
- Effective management of use of cryptographic key techniques during its life cycle.

## 11. Physical and Environmental Security Policy

**Purpose**

The purpose of this policy is to prevent unauthorized physical access, damage and interference to organizational premises and information, to prevent loss or damage to information assets and interruption to business activities and to prevent compromise or theft of information and information assets.

**Responsibilities**

- Administration division is responsible for implementation of controls.
- All employees (including contract employees and service providers) of CodeGen are responsible for adhering to this policy.

### 11.1. Security Areas

#### 11.1.1. Physical Security Perimeter

- CodeGen shall have the following designated zones based on the sensitivity of information processing.

| Security Classification Levels | Areas | Entry Controls |
|---|---|---|
| Top Secret | ▪ Data Centre | ▪ Biometric access |
| Sensitive | ▪ IT Operators Area | ▪ Wear CodeGen ID tags all the time |
| Public | ▪ General Administration Area | ▪ Screened and Cleared at Security point |

- The perimeter of CodeGen's premises containing business information and information processing facilities (i.e. IT Data Center, HR, Finance etc.) should be protected by walls/barriers, and appropriate access control mechanisms.

- The perimeter controls must ensure sufficient security commensurate with the sensitivity of the information systems.
- "Top Secret" areas must be indicated with clear signs (e.g., "Restricted Zone - Authorized Personnel Only").

### 11.1.2. Physical entry controls

- To ensure physical and environmental security of the information processing facilities and information assets, CodeGen shall maintain an appropriate physical security perimeter and physical entry controls (Refer to the table in section 11.1.1. above) for the CodeGen Datacenter.
- Access to all critical information processing facilities will be granted in accordance with the access control procedures. Such access will be logged, securely maintained and regularly reviewed by CodeGen.
- "Top Secret" and "Sensitive" areas must have a physical access control mechanism implemented, which allows only specific authorized people to enter, and must be suitable for the type of area being secured. This may include automated access control devices (biometric devices, proximity card devices, etc.) or suitable lock and keys.
- All employees of CodeGen are authorized to access the "Public" area. However, only specifically authorized employees may enter "Top Secret" and "Sensitive" areas other than as visitors.
- Authorization to enter "Top Secret" and "Sensitive" areas are to be granted only when there is a business or technical reason for the person to enter the premises. Authorization to access "Top Secret" and "Sensitive" areas must be approved by an authorized personnel.
- Visitor access to "Top Secret" and "Sensitive" areas where sensitive information (digital or printed) or information systems are located, should be escorted by an internal staff member.
- Physical access rights must be revoked immediately upon termination / resignation of employees or completion of a consultation or vendor agreement.
- For data center security, names of the approved individuals shall be included in the authorized Personnel list and shall be maintained by the Head of ITD. Only authorized personnel shall be allowed to take any computing devices or removable media inside the data center.
- Unauthorized access into the data center and/or violation of this policy must be reported to CISO, with the date and time and name of the person(s) causing the violation or the information security incident.
- A record of visitor access to "Top Secret" and "Sensitive" areas must be maintained for each location. The records must at minimum contain name and identification of the visitor

(employee number, National ID number / passport number), date and time of entry, reason for the entry, date and time of exit, and name and employee number of authorized employee escorting the visitor. These records may be automated (i.e., logs of access control device), manual (i.e., log book), or a combination of both.

- The ISM must regularly review the records of physical security, for accuracy and consistency.
- External agencies' access such as courier and delivery services shall be restricted to designated delivery/ collection points.

### 11.1.3. Securing Offices, Rooms and Facilities

- CodeGen shall ensure that sensitive and/or critical information processing facilities are appropriately equipped and maintained with security controls to safeguard the information contained within the facility against man made or environmental threats.

### 11.1.4. Protecting Against External and Environmental Threats

**Protection from External Threats**

- Physical safety of personnel must take precedence in any circumstances, and must not be compromised in achieving any other policy objective.
- CodeGen must adhere to all health and safety rules and regulations imposed by the Government and other applicable regulatory bodies.
- Where possible, manned security points shall be implemented at "Top Secret" and "Secret" area entry points.
- CCTV monitoring systems shall be implemented for the above zones. CCTV recording shall enable CodeGen to provide evidence during an information security incident investigation.

**Protection from Fire**

- Fire detection and extinguishing equipment must be placed and must be adequate in order to protect critical business processing equipment. They should be located near critical equipment for easy access.
- CodeGen Administration division is responsible for the selection and maintenance of all fire detection and extinguishing equipment at CodeGen premises.
- Maintenance work of fire detection and suppression equipment must be carried out by persons with required expertise. Frequency of maintenance must be as stipulated by the equipment supplier. Instructions on use of fire extinguishers must be placed close to each fire extinguisher.

- Hazardous or combustible materials should not be kept in or around sensitive areas (e.g., Data Centers, server room, UPS room, etc.). If such material is to be stored in the same premises, they must be kept at a safe distance from the sensitive areas. Fire extinguishers of an appropriate type must be located in close proximity to such material.
- Appointed fire marshals must be trained in the use of all fire extinguishing equipment available to them. The training frequency must be bi annually.
- All employees are responsible to educate themselves on the use of fire equipment and fire safety procedures, and must seek advice and instructions from the Administration division whenever required.

**Protection from Water Damage**

- All IT equipment must be sited to prevent water damage, such as from floods, rain, plumbing defects, etc. Safeguards may include raised floors / keeping equipment on elevated platforms as well as premises design safeguards such as proper drainage systems.

**Power, Air-conditioning, and Other Supporting Utilities**

- All IT equipment must be maintained in conditions within which suppliers warranty continues to be applicable. Whenever applicable, all systems must be maintained as per the guidelines (with regard to power supply, humidity, ventilation, temperature control, etc.) provided by the supplier.
- The power supply system of CodeGen premises must be implemented to provide the required level of safety and continuity. The implementation of the fire suppression system, air-conditioning, and other critical systems must be taken into consideration when designing the power supply system.
- All critical IT systems (including server, network equipment, and workstations) must have sufficient protection for power failures, including power loss, voltage anomalies, etc. Protection measures may include a combination of Uninterruptible Power Supply (UPS) devices and generators. The protection measures must be appropriate with the local main power supply conditions at each location.
- All power supply equipment of CodeGen must be tested and maintained regularly as per the guidelines of the relevant equipment manufacturer. The safeguard and maintenance of such equipment is the responsibility of the building maintenance.
- Whenever the IT equipment requires regulation of air temperature (e.g., for servers), the air-conditioning system to that area must be supplied with uninterruptible power.
- Environmental conditions affecting proper functioning of the IT equipment (such as air temperature and humidity in the server room) must be regularly monitored by the relevant process owners. If any adverse condition is detected, immediate steps must be taken to

avoid data loss and system failure. When evaluating the environmental factors, the equipment and system suppliers' guidelines must be taken into consideration.

#### 11.1.5. Working in Secure Areas

- Working guidelines shall be given for "Top Secret" and "Sensitive" areas which shall be followed by all the CodeGen employees.
- All visitors working in "Top Secret" and "Sensitive" areas must be under the supervision of a person with authorization for that zone. This is especially applicable for maintenance and cleaning work carried out within "Top Secret" and "Sensitive" areas by external parties.
- Vacant "Top Secret" and "Sensitive" areas must be locked and periodically checked by authorized personnel.
- No photographic, video, audio, or other recording equipment should be allowed into "Top Secret" areas without obtaining authorization from the CISO.

#### 11.1.6. Delivery and Loading Areas

- Delivery and loading areas, as well as other publicly accessible areas shall be appropriately isolated from information assets and information processing facilities.

### 11.2. Equipment

#### 11.2.1. Equipment Siting and Protection

- Network devices such as routers, servers, network cables, switches, and hubs must be placed in the "Top Secret" area that provides protection from unauthorized or unnecessary access.
- All data storage devices and backup equipment must be kept in designated secure areas and must not be kept in the "Public" area.
- The location of critical equipment must be reviewed and approved by the CISO, who should consider the safety of the equipment from water, fire, and other environmental damage.

#### 11.2.2. Supporting Utilities

- Adequate mechanisms shall be implemented to protect equipment from power failures and other disruptions caused by failures in supporting utilities. (i.e. Uninterrupted Power Systems and Generators).

#### 11.2.3. Cabling Security

- Network and power cabling should be protected and secured from unauthorized interception and damage. Whenever possible, cabling must be made underground or alternatively within a secured housing.

- Cable and equipment markings and naming should be clearly identifiable and should be documented for reference and to avoid errors or mistakes.
- A network cabling diagram must be maintained by the Network Administrator and Network for all premises of CodeGen covering all data networks of CodeGen.
- Network cabling diagrams should separate from power cabling.

### 11.2.4. Equipment Maintenance

- Equipment should be maintained periodically according to vendor specifications and service intervals.
- The maintenance of equipment should be carried out by authorized personnel only. CodeGen must ensure that maintenance is carried out by persons with the necessary technical competency. CodeGen must also ensure the sufficiency of procedures for the safety of equipment and data during maintenance work.
- Records of equipment failures during maintenance should be kept, along with the remedial measures executed to rectify the failure. The records should include the names and identification of the personnel who took part in the particular maintenance routine.

### 11.2.5. Removal of Assets

- Equipment used to support business activities outside CodeGen must be subject to the same type of management authorization and security protection as that of on-site equipment.
- No person is allowed to remove any IT equipment (including workstations (Desktop), peripherals, and storage media) from CodeGen premises without approval by the CISO. Respective asset owners must maintain a register of all equipment approved for removal from CodeGen premises indicating the person responsible for the equipment, timeframe approved for removal and reasons for removal.
- Removal of data storage devices or equipment with data storage devices must be approved by the CISO.
- The CISO must ensure that all equipment removed from CodeGen custody for maintenance purposes are properly secured and sanitized to prevent unauthorized access to information kept in such equipment.

### 11.2.6. Security of Equipment and Assets Off-Premises

- CodeGen IT management shall ensure that no storage media containing CodeGen information will be sent off premises (outside CodeGen premises) without any approval and shall for the gate pass process.

### 11.2.7. Secure Disposal or Reuse of Equipment

- All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. This shall be handled as per section 8.5.2 Disposal of Media.

### 11.2.8. Unattended User Equipment

- Equipment such as personal computers, servers, terminals and other devices shall be protected from unauthorized use and/or access when unattended.
- Appropriate security measures such as password protected screen savers and/or screen or key locks, automated termination of active sessions shall be adopted to protect the unattended equipment.

### 11.2.9. Clear Desk and Clear Screen Policy

- Documents containing confidential organizational information should be stored in a safe and secure place.
- Every employee should ensure that whenever they leave their desk, they lock their screen and clear all documents from their respective desks.
- The white boards/ flip charts used by the users shall also be cleared and no critical information shall be left on the boards / flip charts.
- Sensitive information shall be turned over or shall be put out of sight when visitors are present.
- Disposal of paper documents and storage media shall follow the approved guidelines.
- Remember that it is a fundamental principle that knowledge or possession of sensitive information is to be strictly limited to those users that have a need to know and appropriate privileges; CodeGen users are to adhere to this principle.
- All employees must follow CodeGen clear desk and clear screen policy instructions.

## 12. Operations Security

**Purpose**

The purpose of this policy is to have a framework for providing secure operations for information systems and facilities of CodeGen.

**Responsibilities**

**ISSC:** Is responsible for ensuring adequate resources for systems / network security and availability.

**Chief Information Security Officer (CISO):** Is responsible for:

- Developing, documenting and maintaining the operating procedures related to CodeGen's information facilities and communication systems.
- Periodically reviewing the process of movement of information, media, storage and disposal.
- Periodic review of user logs, wherever required.

**System Owners/Administrators:** are responsible for implementing and maintaining operating procedures:

- Implementing approved changes
- Backup procedures
- Capacity Management

**IT Infrastructure Team:** Is responsible for the following operations

- Network security management
- Performance Management

**End User:** Is responsible for the following activities:

- Periodic backup on their own.
- Adherence to Acceptable Usage Policy.

### 12.1. Operational Procedures and Responsibilities

#### 12.1.1. Documented Operating Procedures

- Operating procedures to enforce all components and requirements of the CodeGen Information Security Policy Manual and Supplementary Security Policies shall be maintained and updated by CodeGen.
- Operating procedures for information systems shall be documented and authorized by the management. These procedures shall include:
  - Server and networking equipment start up and close down;
  - Backup;
  - Equipment maintenance; and
  - Media handling.
- Operating procedures require specifying the instructions for the detailed execution of each job including the interdependencies if any and instructions for dealing with exceptions or errors that may arise during job execution.

#### 12.1.2. Change Management

- Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all changes to equipment, operating systems, application software, and procedures are required to be followed.

- Changes to systems and infrastructure shall be duly approved before implementation and a risk assessment shall be carried out.
- A ticket shall be raised in the Change management system for each scheduled, unscheduled or business critical change following the steps contained in the ***Infrastructure Change & Release Management Procedure***
- A change review shall be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A change management log shall be maintained for all changes. The log must contain, but is not limited to:
    - Date of submission and date of change
    - Owner and custodian contact information
    - Identification and nature of the change
    - Results of testing of changes
    - Assessment of potential impacts and security risks
    - Indication of success or failure
    - Communication of change details to all relevant parties
- Fall back procedures should be clearly defined for aborting and recovering from unsuccessful changes.

### 12.1.3. Capacity Management

- Capacity management shall be carried out by respective division heads for their information assets considering the current utilization and future capacity requirements following the ***Performance Availability and Capacity Management Procedure (PR-CG-ISMS-010)***. This includes capacity management for following (not limited to):
    - Hardware resources;
    - Software licensing;
    - Network bandwidth;
    - Workstations;
    - Storage;
    - Processing;
    - Data center space; and
    - Personal or human resources.
- Performance of critical information processing and communication facilities shall be monitored.
- The performance monitoring reports shall be analyzed and any bottlenecks shall be identified. For each new and ongoing activity, capacity requirements shall be identified.

System tuning and monitoring shall be carried out to ensure and, where necessary, improve the availability and efficiency of the systems.

- Head of ITD shall use this information to identify and avoid any potential bottlenecks that might present a threat to system or services, and plan appropriate action.

#### 12.1.4. Separation of Development, Testing and Operational Environments

- Development, test and operational facilities shall be separated to reduce the risks from unauthorized access or (inadvertent) changes to the operational systems.
- The level of separation between operational, test, and development environments that is necessary to prevent operational problems shall be identified and appropriate controls implemented.
- Rules for the transfer of software from development to operational status shall be defined and documented.
- Users shall use different user profiles for operational and test systems, and menus shall display appropriate identification messages to reduce the risk of error; and sensitive data shall not be copied into the test system environment.

### 12.2. Protection from Malware

#### 12.2.1. Controls against Malware

**Detection**

- The symptoms of malicious software infections include considerably slower response from the system, inexplicable loss of data, erroneous change in file dates, increase or decrease in file size or total failure of the computer system.
- End users shall report these kinds of abnormal behaviors of the system, immediately to the ITD. ITD will follow ***Information Security Incident Management Procedure (PR-CG-ISMS-008)*** to respond to the incident.

**Protection and Treatment**

Necessary technical and operational procedures shall be in place for centralized antivirus definition updates.

- It shall be ensured that the anti-virus software is installed and active on every PC. The configuration of anti-virus software shall be protected to avoid any unauthorized modifications.
- Updating of anti-virus definitions on all desktops shall be managed centrally. Antivirus software/scanning engine shall also be updated as per software vendor's recommendations.

- Systems shall be implemented to review the anti-virus software activity / logs, to check whether anti-virus software is running regularly on respective computers.
- Machines shall be scanned for viruses on predetermined intervals.
- Every diskette, CD and any storage media shall be scanned for virus before use.
- Controls shall be implemented to protect the network from spyware malicious applications.
- The Anti-Virus software for messaging system (e-mail) shall be implemented. If a virus is found in a mail attachment file, this file shall be deleted and the sender will be informed. The recipient would get the remaining message.
- Users shall be regularly updated about the latest information on malicious code through circulars, internal magazines or IT communications etc.
- Unauthorized or any pirated software shall not be used by the CodeGen employees.
- Any files or data obtained from outside through any media required for business, shall be tested for viruses before being used.
- Appropriate recovery procedure shall be in place for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements.
- Necessary procedural protection shall be taken to protect against the introduction of malicious code during maintenance and emergency procedures, which may bypass normal malicious code protection controls.

**Employee Responsibility**

- CodeGen employees should ensure that their PCs are kept virus free by actions such as not opening email attachments from unknown sources.
- If CodeGen employees are authorized to use removable media such as CDs and Flash drives, ensure that they are scanned before use.

**Exceptions**

- Antivirus updates on workstations that are kept switched off due to unavailability of the user shall be updated at the next workstation startup.
- Antivirus scans on workstations that are kept switched off due to unavailability of the user shall be carried out during the next scheduled scan.
- Unmanaged computers will be exempted from this policy.

### 12.3. Backup

#### 12.3.1. Information Backup

- Information asset owners are responsible to maintain an appropriate backup plan and schedule for their respective information assets as per the business requirements and following the ***Backup and Recovery Procedure (PR-CG-ISMS-007).***
- Onsite and offsite backup storage sites shall be appropriately protected.

## 12.4. Logging and Monitoring

### 12.4.1. Event Logging

- System Administrator shall maintain Operational and Maintenance logs of all activities.
- The logging shall be automated as far as possible. Implement automatic recording of logs wherever feasible as it is useful to maintain the integrity of the logged information. Logs shall include but not limited to;
    - Date, time and other details of key events, e.g. log-on and log-off
    - Records of successful and rejected system access attempts
    - Changes to system configuration
    - Use of privileges

**Fault Logging**

- Users must report to the CodeGen of all incidents in which the system is unable to function as required.
- CodeGen must maintain a complete log of all reported faults (which is separate and different from the change request log), reported by users, third parties, or discovered in any other manner. The fault log must include the nature of fault, affected systems, identified cause, and corrective measures taken.
- System error logs and solutions provided shall be reviewed periodically by the Internal/External Auditors.

**Review of Logs**

- Head of ITD shall review the logs at least once a month to initiate timely actions for system or network errors. Regular review of the logs is essential to maintain maximum uptime of the system, which leads to continuity of business process.
- ISM shall conduct periodic reviews of logs. These reviews are helpful in ensuring that operating procedures are performed properly and information security controls are effective.

**Monitoring System Use**

- System Administrator shall monitor the use of information systems to safeguard the information from unauthorized activities.
- Level of monitoring shall be determined by risk assessment of individual systems.
- Review of event logs is an important function in monitoring system use. System Administrator shall monitor their respective systems at least once a month and report any unauthorized activity noticed. Head of ITD and the ISM shall be notified about the same.

#### 12.4.2. Protection of Log Information

- Logs shall be protected from unauthorized accesses and changes.
- Logs shall be backed up daily. These logs shall be archived quarterly for all critical systems.
- The log retention period shall be determined based on business needs, legal, statutory and contractual obligations.

#### 12.4.3. Administrator and Operator Logs

- All activities of the system operator shall be reviewed at least once in a quarter by the ISM.

#### 12.4.4. Clock Synchronization

The correct setting of computer clocks is important to ensure accuracy of logs. The logs may be required for investigations or as evidence in legal or disciplinary process.

- All information systems and devices wherever applicable, which have real time clocks, shall be set to Sri Lankan Standard Time Zone (GMT+5:30).
- System Administrator shall regularly check and maintain the clocks using an NTP server as per standard time settings as mentioned above.

### 12.5. Control of Operations Software

#### 12.5.1. Installation of Software on Operational Systems

- To minimize the risk of corruption to the operational systems, the procedures shall be in place to control the installation of software.
- The business requirements for the change shall be taken into account before upgrading software to a new release.
- The risks and severity of security problems affecting the new version shall be considered before change or maintenance.
- Updates to operational software, applications, and program libraries shall only be performed by appropriately trained personnel following management authorization.
- Operational systems shall only hold approved executable code, and not development code or compilers.
- Applications and operating system software should only be implemented after extensive and successful testing; the tests may include tests on usability, security, effects on other systems and user-friendliness, and should be carried out on separate systems (non-production environment).
- A roll back strategy shall be in place prior to implementing changes to the production environment.
- An audit log shall be maintained of all updates to the customization table.

## 12.6. Technical Vulnerability Management

### 12.6.1. Management of Technical Vulnerabilities

- To minimize the risks from operating system changes, business critical applications and systems shall be reviewed and tested to ensure that there is no adverse impact on the organizational operations or security of those applications or operating systems.
- Adequate responsibilities shall be established within the organization for implementing and monitoring vulnerabilities and vendor's release of patches and fixes.
- CodeGen shall establish a technical vulnerability management process with defined frequencies and a scope. These will include but not limited to
  - External vulnerability testing for internet facing servers;
  - Internal vulnerability testing for critical application servers;
  - Web application vulnerability test (if required); and
  - Firewall configuration reviews.
- Timely information about technical vulnerabilities of information systems shall be obtained by CISO via the special interest groups and communicated to relevant information asset owners.
- CodeGen's exposure to such vulnerabilities shall be evaluated, and appropriate countermeasures will be defined and implemented in a timely manner, to address the associated risks.

**Patch Management**

All system components directly associated with CodeGen data environment must be securely hardened and configured with all necessary and appropriate patches and system updates for preventing the exploitation or disruption of mission-critical services. All patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing and verifying.

Patch Management will consist of:

- Subscribing to industry-leading security sources, additional supporting resources for vulnerability announcements and other security patch management alerts and issues
- Procedures for establishing priorities regarding Security Patch Management. This will include, but is not limited to (1) the significance of the threat, (2) the existence and overall threat of the exploitation and (3) the risks involved in applying Security Patch Management procedures (its effect on other systems, resources available and resource constraints).
- Procedures for the deployment, distribution and implementation of patches and other related security-hardening procedures.

- Process owners shall verify that the patches are tested and successfully deployed.

### 12.6.2. Restrictions on software installation

- Rules governing the installation of software by users shall be established and implemented.
- The organization shall define and enforce strict policy on which types of software users may install.
- The principle of least privilege shall be applied. If granted certain privileges, users may have the ability to install software. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose category with regard to being potentially malicious is unknown or suspect). These privileges shall be granted having regard to the roles of the users concerned.

## 12.7. Information Systems Audit Considerations

### 12.7.1. Information Systems Audit Controls

- ISSC shall define the scope of information systems audit and identify the resources required for performing it.
- Persons carrying out the audit shall have proficiency in audit and will be independent of the work to be audited.
- All access to information and information systems provided to auditors shall be read only.

**Protection of Information Systems Audit Tools**

- Audit tools shall be adequately protected from tampering and modifications.
- These tools shall have restricted access and auditee access to these tools will be prohibited.
- Wherever the third party is assigned to perform the audit, risks from misuse of these tools shall be appropriately addressed and necessary approval shall be sought before performing the system audits.

# 13. Communications Security

**Purpose**

The purpose of this policy is to ensure the protection of information in networks and its supporting information processing facilities.

**Responsibilities**

**Chief Information Security Officer (CISO):** shall be responsible in implementing the specific controls that are given in this policy.

### 13.1. Network Security Management

#### 13.1.1. Network Controls

- Appropriate logical and physical security measures and features shall be implemented to protect the network.
- System administrators must establish appropriate controls to prevent unauthorized access that could impact critical business information assets within the network and connected services.
- Controls must be implemented to protect connected systems, and to safeguard the confidentiality and integrity of critical business information assets that pass over public networks.
- Appropriate network security requirements must be covered by the Service Level Agreements (SLA) with external parties.

**Access to Network Infrastructure and Utilities**

- Logical access to networking hardware and software must be limited to properly authorized personnel.
- Access to programmable network devices (e.g., routers, switches and bridges) must be restricted to authorized ITD staff.
- The use of network diagnostic and security tools must be limited to specifically designated staff, and in accordance with their job responsibilities.
- Access to all network configuration and security-related data, must be limited to authorized users.

**General Network Management Controls**

- Network infrastructure devices must be configured to prevent the disclosure of the configuration of the internal network to external entities.
- Unattended network connection ports (e.g., conference rooms, empty offices, etc.) must be enabled only when needed, and must be blocked at all other times.
- Any services that are not required must be blocked, preferably at the firewall, and where possible, also at the end system or server.
- Users must only be provided with direct access to the services that they have been specifically authorized to use.

**Network Infrastructure Management Controls**

- The System Administrator shall request permission via change request from the CISO prior to performing any alteration on CodeGen network security standards.
- CISO shall approve any modification on CodeGen network prior to implementation.
- The System Administrator shall maintain a record of files pertaining to a network security change in soft copy format including but not limited to the approval of the CISO, recommendations, consultancy records, etc.
- The System Administrator shall maintain an updated network diagram and a copy shall be provided to the CISO.
- The System Administrator shall perform network policy alterations with authorization of CISO and shall keep a record, documentation and reasons that lead to the network alteration.

### 13.1.2. Security of Network Services

- CodeGen shall regularly monitor the ability of the network service providers to manage agreed services in a secure manner.
- The security arrangements necessary for particular services, such as security features of network services, service levels, and management requirements, should be identified where necessary. CodeGen shall ensure that network service providers implement these measures.

### 13.1.3. Segregation in Networks

- CodeGen shall segregate the network to isolated networks to prevent unauthorized access.
- Networks shall be appropriately segregated using an appropriate mechanism.
- User access to production servers shall be restricted to the presentation layer of the applications and based on known application ports.

## 13.2. Information Transfer

### 13.2.1. Information Transfer Policies and Procedures

- Appropriate controls shall be implemented for protection against malicious code, while transmitting information electronically.
- Sensitive information shall be protected using encryption, password or any other suitable method especially when being sent as an attachment in an email.
- Disposal procedures shall be followed to destroy sensitive information.
- End users will:
    - Not leave sensitive information unattended at fax machines, printers, etc.

- Not auto-forward mails to external mail ids.
- Not reveal sensitive information in public
- Not leave sensitive messages on answering machines
- Check the recipients email id/fax number before sending an email or a fax respectively.

### 13.2.2. Agreements on Information Transfer

- In case of an exchange of information between CodeGen and an external party, appropriate agreement shall be established addressing the following points:
  - Traceability and non-repudiation;
  - Courier identification standards;
  - Responsibilities and liabilities in the event of an incident;
  - Labelling system as per the sensitivity of the information; and
  - Cryptography.

### 13.2.3. Electronic Messaging

- Information present in electronic messages shall be appropriately protected according to its criticality.
- Confidential Emails shall be encrypted and attachments shall be password protected for information passing over the publicly accessible networks.

### 13.2.4. Confidentiality or Non-Disclosure Agreements

- Confidentiality agreements shall be signed between parties where any CodeGen information exchange is applicable.
- The standard agreement template approved by CodeGen legal shall be used.
- Periodic review shall be carried out to include any potential risks, addressed and documented by CodeGen legal team.

## 14. System Acquisition, Development and Maintenance Policy

**Purpose**

The purpose of this policy is to ensure that security is built into information systems during development; access is restricted to system files; source codes are appropriately controlled; unauthorized modification or misuse of application data is prevented; and security of application systems is maintained.

**Responsibility**

**CISO / System Owner:** shall be responsible for identifying security requirements before initiating any development and maintenance activities on any information processing system and change in the existing system within CodeGen.

### 14.1. Security Requirements of Information Systems

#### 14.1.1. Information Security Requirements Analysis and Specification

- The evaluation of the security of new systems or software will be done with the ISSC and respective leads. The evaluation will consider the security requirements of the new systems after performing a risk assessment.
- When any system or software is procured, the product and vendor is evaluated based on the business needs, and CodeGen standards and requirements. This evaluation criterion will include appropriate security related considerations including input validations, process integrity controls and output validations.
- The evaluation of software packages shall also take into consideration automated controls as well as their capabilities to support manual controls.
- Security requirements and controls considered shall be in-line with the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security.
- Information security requirements shall be integrated throughout the system development or integration project lifecycle, from initiation to completion.
- Contracts with the supplier shall address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, then the risks introduced and associated controls shall be reconsidered, prior to purchasing the product.
- Where additional functionality supplied with a product causes additional security risks, these additional functionality should be disabled or the proposed control structure should be reevaluated to determine if advantages can be gained from the enhanced functionality.
- Following will be considered at a minimum when purchasing new information systems.
    - User access mechanisms and controls related to user management;
    - Password related controls;
    - Logging mechanism;
    - Error handling methods; and
    - Database related security features.

### 14.1.2. Securing Application Services on Public Networks

- Any application services which will be hosted on public servers or communication involving passing information over public networks shall undergo thorough vulnerability assessments, penetration testing and quality assurance to ensure the adequacy of controls to mitigate threats applicable to such applications.

### 14.1.3. Protecting Application Services Transactions

- ITD shall ensure information involved in application service transactions are protected using adequate controls to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

## 14.2. Security in Development and Support Processes

### 14.2.1. Secure Development Policy

- Widely accepted secure software development guidelines shall be used in developing systems.
- CodeGen shall apply appropriate controls to prevent opportunities for information leakage. Such controls include considerations for the regular monitoring of personnel activities, system activities and resource usage.
- Rules for development of software and systems shall be established using an adequate methodology and applied to software developments.
- In the event software development is outsourced, applicable controls and rules shall be communicated promptly to the outsourced vendor and contractually agreed. CodeGen shall closely monitor the outsourced software development for their adherence to the agreed terms.

### 14.2.2. System Change Control Procedures

- To minimize the risk during system development and maintenance, the implementation of changes shall be controlled according to the ***Infrastructure Change & Release Management Procedure***.
- Adequate risk analysis, analysis of impacts of those changes affecting the systems, and mitigating the risks arising out of such changes shall be documented and records of change implementation be maintained.

### 14.2.3. Technical Review of Applications after Operating Platform Changes

- To minimize the risks from operating system changes, business critical applications and systems shall be reviewed and tested to ensure that there is no adverse impact on the organizational operations or security of those applications or operating systems.
- Adequate responsibilities shall be established within the organization for implementing and monitoring vulnerabilities and vendor's release of patches and fixes.

### 14.2.4. Restrictions on Changes to Software Packages

- Modifications to purchased software shall be restricted and if required shall be implemented through ***Infrastructure Change & Release Management Procedure***

### 14.2.5. Secure system engineering principles

- Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.
- Secure information system engineering procedures based on security engineering principles shall be established, documented and applied to in-house information system engineering activities. Security shall be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology shall be analyzed for security risks and the design shall be reviewed against known attack patterns.
- These principles and the established engineering procedures shall be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They shall also be regularly reviewed to ensure that they remain up-to-date in terms of combating any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.
- The established security engineering principles shall be applied, where applicable, to outsourced information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources. The organization shall confirm that the supplier is in compliance with CodeGen's secure system engineering principles.

### 14.2.6. Secure Development Environment

- CodeGen shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

### 14.2.7. Outsourced Development

- Wherever the software development is outsourced, the development shall be supervised and monitored. Adequate procedures or process shall be in place for licensing agreements, code ownership, and intellectual property rights, quality assurance on the software developed, testing before implementation etc.

### 14.2.8. System Security Testing

- Testing of security functionality shall be carried out during development.
- New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions.

- All software changes shall be documented and approved by authorized personnel.
- All modifications to software packages shall be strictly controlled with approval by authorized personnel.

#### 14.2.9. System Acceptance Testing

- For all the new information systems, upgrades to existing systems or new versions, acceptance criteria shall be clearly defined prior to testing and shall be approved by the business owners.
- System shall not be allowed to be released to the production environment until the testing is complete and the user sign off obtained for all the test results.
- The CISO shall be consulted in order to define the criteria relating to information security.
- A detailed checklist shall be prepared for various parameters to be incorporated in the acceptance test. The acceptance criteria can be based on process requirements and/or user requirements.

### 14.3. Test Data

#### 14.3.1. Protection of Test Data

- To minimize the risks from test data, the data shall be selected carefully, protected and controlled.
- The use of operational databases containing personal information or any other sensitive information for testing purposes shall be avoided.
- The following guidelines shall be applied to protect operational data, when used for testing purposes;
- The access control procedures which apply to production environment, shall also be applicable to testing environment (test application systems);
- The authorization procedure shall be followed for each time whenever operational information is copied to test application system;
- The operation/production data shall be erased after its use from testing application system; and
- Logs of production system data copying to testing systems shall be maintained.

## 15. Supplier relationships

**Purpose**

The purpose of this policy is to maintain an agreed level of information security and service delivery in line with supplier agreements.

**Responsibility**

**CISO/ System Owner:** shall be responsible for ensuring compliance to this policy where applicable to IT Operations.

## 15.1. Information Security in Supplier Relationships

### 15.1.1. Information Security Policy for Supplier Relationships

- CISO shall be responsible to conduct a risk assessment to identify potential risks to CodeGen's Information Security as a result of service provisioning through third party. This shall be carried out with the assistance of the information security manager, respective project managers and CodeGen Legal Officer.
- This risk assessment should consider the following criteria:
    - The type of information or data processing functions or services to be accessed by a third party;
    - The risk classification of the information or data processed by the systems that third party will be working with; and
    - Background information about the third party.
- Based on the risk assessment results, information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented in the form of an agreement.

### 15.1.2. Addressing Security within Supplier Agreements

- Supplier contracts must be consistent in all respects with CodeGen's Information Security Policies and Procedures.
- Supplier contracts must include the following conditions, as applicable:
    - Description of the information to be provided or accessed;
    - The level of physical and logical security that will be provided (by the third party) to maintain the confidentiality, integrity and availability of the information to be provided or accessed;
    - Classification of the information. Classification scheme can be CodeGen's information classification scheme or an acceptable scheme agreed by both parties;
    - The service level to be provided and the level of availability in the event of a disaster;

- Provision for confidentiality, non-disclosure and acceptable use relating to the information /data processed by the outsourced function or service;
- Legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;
- Rules of acceptable use of information, including unacceptable use if necessary;
- Information security policies relevant to the specific contract;
- Incident management requirements and procedures (especially notification and collaboration during incident remediation);
- Training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures;
- Relevant regulations for sub-contracting, including the controls that need to be implemented;
- Relevant agreement partners, including a contact person for information security issues;
- Right to audit the supplier processes and controls related to the agreement;
- Defect resolution and conflict resolution processes;
- Supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
- Supplier's obligations to comply with the organization's security requirements;
- Personal screening process for the outsourced staff; and
- Continuity arrangements.

**15.1.3. Information and Communication Technology Supply Chain**

- In certain circumstances CodeGen suppliers may hire another subcontracting party to deliver the services required. In such a situation, it is the responsibility of the main supplier to indicate their supplier chain to CodeGen prior to signing the agreements.
- In such a situation CodeGen shall assess the risk of supplier sub-contracting the services hence risk management plan should be devised accordingly.
- The respective project manager shall validate the sub-contracting party also a known party and a verification of the vendor shall also be carried out.

- Apart from the conditions listed in 15.3.2 Addressing security within Supplier Agreements, following shall be considered for inclusion in supplier agreements concerning supply chain (suppliers of the supplier) security, as applicable:
    - It is the responsibility of the supplier (whom CodeGen is signing the agreement with) to ensure that the sub-contractors are aligning to the information security requirements of CodeGen. This shall be stated in the agreement clearly and supplier will be held responsible for any violations if occurred;
    - A monitoring process on how CodeGen will validate the delivered information and communication technology products and services are adhering to stated conditions in the agreement; and
    - Applicability of the NDA and right to audit requirement for the sub-contractor.

## 15.2. Supplier Service Delivery Management

### 15.2.1. Monitoring and Review of Supplier Services

- Supplier services shall be monitored and reviewed on a timely basis by relevant departments at CodeGen.
- This should involve a service management relationship process between CodeGen and the supplier to:
    - Monitor service performance levels to verify adherence to the agreements;
    - Review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;
    - Conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;
    - Provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;
    - Review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
    - Resolve and manage any identified problems;
    - Review information security aspects of the supplier's relationships with its own suppliers; and

- Ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

### 15.2.2. Managing Changes to Supplier Services

- Any changes to the contract shall be managed depending on the criticality of the service provisioning.
- Changes shall undergo a risk assessment, considering the impact that the change would make to the existing service provisioning and information security posture. Risk treatment options should be planned accordingly and shall be addressed in the revised agreements.

## 16. Information Security Incident Management Policy

**Purpose**

The purpose of this policy is to build an effective system to handle the information security related events and incidents, and to communicate any weaknesses, improvements in the system towards taking timely remedial actions.

Information security incident mean any attempt at, or occurrence of, unauthorized acquisition, exposure, disclosure, use, modification or destruction of data that compromises the Availability, Confidentiality or Integrity of CodeGen's confidential business information and/or CodeGen’s customer data.

**Responsibility**

**Chief Information Security Officer (CISO):** is responsible for implementing incident response procedure. CISO shall supervise and monitor the incident response process.

**Incident Response Team (IR Team):** Responsible for responding to security incidents reported by end users and shall report unresolved incidents to CISO. Incident Response Team will consist of the entire ITD team which includes the following:

- Head of ITD
- Assistant Manager ITD
- Lead / Senior System Administrator
- System Administrators
- Associate System Administrator

- Trainee System Administrator

**End User:** Every person in CodeGen is responsible for reporting the security incident to the ITD by raising Jira tickets or emailing to **itsd@codegen.net** as appropriate.

### 16.1. Management of Information Security Incidents and Improvements

#### 16.1.1. Responsibilities and Procedures

- CodeGen shall establish an Information ***Security Incident Management procedure*** to handle different types of information security incidents.
- In addition to normal contingency plans, the procedures should also cover:
  - Analysis and identification of the root cause of the incident;
  - Containment;
  - Planning and implementation of corrective action to prevent recurrence, if necessary;
  - Communication with those affected by or involved with recovery from the incident; and
  - Reporting the action to the appropriate authority.
- Audit trails and similar evidences shall be collected and secured, as appropriate, for:
  - Internal problem analysis;
  - Forensic evidence in relation to a potential breach of contract or regulatory requirement or in the event of civil or criminal proceedings; and
  - Negotiating for compensation from software and service suppliers.
- Action to recover from security breaches and system failures shall be carefully and formally controlled. The ***Information Security Incident Management Procedure (PR-CG-ISMS-008)*** shall ensure that:
  - Only clearly identified and authorized personnel are allowed access to live systems and data;
  - All emergency actions taken shall be in line with the approved change management policies and procedures and shall be documented in detail; and
  - The integrity of business systems and controls is confirmed with minimal delay.
- Responsibilities of information security incident management shall be clearly communicated to the involved parties and CodeGen shall ensure that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

### 16.1.2. Reporting Information Security Events

- CodeGen users shall report information security events as soon as possible to the ITD.
- Types of information security incidents that may include, but are not limited to the following:
    - Unauthorized access to CodeGen information processing facilities;
    - Misuse of information assets;
    - Unauthorized disclosure of information;
    - Falsification of information;
    - Malicious code and hacker intrusion;
    - Destruction and damage to information assets;
    - Theft/loss/misplace of information, computer equipment or information services;
    - Unavailability of critical information asset;
    - Installation of equipment not authorized by CodeGen ; and
    - Complaint by a customer or a third party.
- Upon receiving the information security incident from the user, respective division heads shall follow the ***Information Security Incident Management Procedure (PR-CG-ISMS-008)*** and self-assign based on the type, nature and severity of the incident.
- ***Information Security Incident Management Procedure (PR-CG-ISMS-008)*** will include identifying an information security incident, reporting methods, incident classification, escalation matrix and incident management.

### 16.1.3. Reporting Information Security Weaknesses

- CodeGen users shall also report any security weaknesses related to systems and services to the information security incident reporting channels in order to prevent such weakness converting into an Information Security Incident.
- CodeGen needs to provide ongoing awareness to the users on identifying information security events and reporting such events to the appropriate parties.
- Contractors and third parties are also required to inform any information security incident or weakness to the respective Project Manager or Team Lead.

### 16.1.4. Assessment of and decision on information security events

- Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

- The point of contact shall assess each information security event using the agreed information security event and incident classification scale and decide whether the event should be classified as an information security incident. Classification and prioritization of incidents help to identify the impact and extent of an incident.
- Results of the assessment and decision shall be recorded in detail for the purpose of future reference and verification.

### 16.1.5. Response to information security incidents

- Information security incidents shall be responded to in accordance with the CodeGen ***Information Security Incident Management Procedure (PR-CG-ISMS-008).***
- Information security incidents shall be responded to by designated personnel and other relevant persons of the organization or external parties.
- The response should include the following:

  a) Collecting evidence as soon as possible after the occurrence;

  b) Conducting information security forensics analysis, as required;

  c) Escalation, as required;

  d) Ensuring that all involved response activities are properly logged for later analysis;

  e) Communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;

  f) Dealing with information security weakness (es) found to cause or contribute to the incident;

  g) Once the incident has been successfully dealt with, formally closing and recording it; and

  h) Post-incident analysis should take place, as necessary, to identify the source of the incident.

### 16.1.6. Learning from Information Security Incidents

- All data that is collected regarding each incident shall be analyzed to identify recurring and/or high impact incidents, and captured within the Information Security Event Log.

#### 16.1.7. Collection of Evidence

- In the event of a security incident originated by an employee or third party, the associated evidence shall be collected and preserved, irrespective of whether a legal action is required or not. They are used to invoke appropriate disciplinary actions as per the HR disciplinary action procedure.
- Whenever applicable, evidence shall be collected by an authorized person or a third party nominated by the management and proper chain of custody has to be maintained.

## 17. Information Security aspects of Business Continuity Management

**Purpose**

The purpose of this policy is to maintain information security continuity embedded into the organization's Business Continuity Management System (BCMS).

**Responsibility**

**Business Continuity Management Committee (BCMC):** Shall nominate members from various departments for the recovery operations and emergency response in case of disaster. Shall also approve and review the business continuity plan, related testing results and policies and procedures.

**IT Division heads:** Shall be responsible for ensuring that a business impact analysis and risk assessment for their respective business process is conducted.

**The BCP Team Leader:** shall be responsible for documenting, maintaining, testing and updating the Business continuity plan and invoking the BCP in the event of a disaster with due approval of the BCMC.

**The Individual BCP Team Members:** Shall be responsible for supporting the business continuity plan, participate in plan testing and recovery processes.

**The System Administrator and Network Administrator:** Shall be responsible for documenting configurations, technical details and restoration procedures for critical information assets.

### 17.1. Information security continuity

#### 17.1.1. Planning Information Security Continuity

- CodeGen BCMC shall include the information security aspects during the business process and technology recovery.

- CodeGen shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
- BCP and DRP testing shall also include the information security continuity testing and results shall be submitted to BCMC and ISSC.

#### 17.1.2. Implementing Information Security Continuity

- Business continuity plans (BCP) and Disaster recovery plans (DRP) shall include the information security requirements to consider during the crisis and recovery times and maintain the continuity of information security management in adverse situations.
- According to the information security continuity requirements, the organization should establish, document, implement and maintain:
    - Information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;
    - Processes, procedures and implementation changes to maintain existing information security controls during an adverse situation; and
    - Compensating controls for information security controls that cannot be maintained during an adverse situation.

#### 17.1.3. Verify, Review and Evaluate Information Security Continuity

- BCP and DRP testing shall also include the information security continuity testing and results shall be submitted to BCMC.

### 17.2. Redundancies

#### 17.2.1. Availability of Information Processing Facilities

- CodeGen shall implement High Availability (HA) solutions for business critical information assets to ensure continued services.

## 18. Compliance

**Purpose**

The purpose of this policy is to mitigate the risk of breaches of any criminal or civil law, statutory, regulatory or contractual obligations, and of any security policies; to ensure compliance of information processing systems with the security policy and standards; and to minimize interference to business operations from system audit process by appropriate planning.

**Responsibilities**

**End Users**: CodeGen employees are responsible for adhering to security policies and procedures.

### 18.1. Compliance with Legal and Contractual Requirements

#### 18.1.1. Identification of Applicable Legislation and Contractual Requirements

- ISM shall maintain a list of laws, statutory, regulatory and contractual requirements applicable to CodeGen in relation to information security with the consultation of CodeGen legal and compliance divisions.
- This list shall be circulated to ISSC, and copy of such laws, acts, and regulations shall be maintained in a central repository by Legal.

#### 18.1.2. Intellectual Property Rights (IPR)

- Compliance with legal restrictions shall be ensured on the use of material for which there may be intellectual property rights, such as copyrights, trademarks etc. All legislative, contractual or regulatory restrictions on the usage and copying of proprietary material shall be adhered to.
- The usage and copying of software products shall be restricted as per the terms and conditions of licensing agreement. An inventory of all software product licenses shall be maintained and usage of unlicensed software in its Information System shall be strictly avoided.

❖ **CodeGen Personnel shall abide by the Intellectual Property Act No. 36 of 2006 (as amended) with regard to licensing agreements of software and hardware.**

- Personnel shall not copy and distribute the proprietary computer software' and materials.
- CodeGen Personnel shall not use unlicensed software on Computer Equipment and Information Resources.
- It is the responsibility to obtain appropriate licenses for the use of software on Computer Equipment and Information Resources.
- CodeGen should ensure compliance with maintaining appropriate license conditions by not exceeding the permitted maximum number of users as stated in the respective agreements.
- Resale or donation of old or redundant computer equipment should be carried out after removing all the copyright software which is under licensed agreements.
- CodeGen shall respond to all appropriate notices of copyright infringement and violations.

### 18.1.3. Other Applicable Legislations

❖ **CodeGen Personnel shall abide by the Computer Crimes Act (CCA) No 24 of 2007.**

- Access any computer or any information held in any system, knowing that he/she has no lawful authority to secure such access;
- Do any act to secure for himself/herself or for any other person access to any computer or any information held in any computer, which he/she has no lawful authority to secure and with the intention of committing an offence under the CCA or any other law;
- Cause a computer to perform any function which will result in unauthorized modification or damage to any computer or computer system or computer program;
- Cause any computer to perform any function which will result in danger to the national security, the national economy or public order;
- Buy, Sell, download, upload, copy or acquire the substance or meaning of any information or in any manner deal with any information obtained from a computer or a storage medium of a computer;
- Intercept any subscriber information or traffic data or any communication, to, from or within a computer or any electromagnetic emissions from a computer that carries any information;
- Sell, procure for use, import, export, distribute or otherwise make available any device, (including a computer or computer program), computer password, access code or similar information by which a computer is capable of being accessed, with the intent that it be used by any person for the purpose of committing an offence;
- Disclose any information which has been entrusted with, which enables him/her to access any service provided by means of a computer.

❖ **Convention on the Suppression of Terrorist Financing Act No. 25 of 2005 and Prevention of Money Laundering Act No. 5 of 2006. Financial Transaction Reporting Act No. 6 of 2006 and the FIU regulations**

- CodeGen Personnel shall ensure at all times that they refrain from doing any act through the internet, email or through the computer equipment and information resources of the company which will amount to an offence under the above Acts or regulations.

❖ **Electronic Transactions Act No.19 of 2006 and Evidence Ordinance of 1995.**

- Employees should when corresponding with third parties ensure that they do not make any statements or undertakings which may be construed by the other party to infer legal obligations on the company since as per the above Act , an offer, and the acceptance of an offer may be expressed in electronic form and that contract shall not be denied legal validity or enforceability on the sole ground that it is in electronic form whilst the Evidence Ordinance paves the way for computer data to be accepted as evidence in a court of law.

❖ **General Data Protection Regulation**

- GDPR mandates a baseline set of standards for organizations that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data. Some of the key privacy and data protection requirements of the GDPR include:
  I. Requiring the consent of subjects for data processing
  II. Anonymizing collected data to protect privacy
  III. Providing data breach notifications
  IV. Safely handling the transfer of data across borders
  V. Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

❖ **ISO 27001:2013 Information Security Management System**

- ISO 27001:2013 is an Information Security Management System framework and this framework will be applicable to the CodeGen processes. ISO 27001:2013 consist of 114 controls and all the controls are applicable to the CodeGen;
  I. Increased reliability and security of systems and information
  II. Increased business resilience
  III. Improved management processes and integration with corporate risk strategies
  IV. Increasing the overall security maturity of the business.
  V. Compliance with Legal, Contractual and regulatory requirements and responsibilities

**18.1.4. Protection of Records**

- No cardholder data including PAN, CVV, PIN, Track Data will be stored within CodeGen network and systems or transmitted using end user messaging technologies.

- Important records shall be protected from possible loss, destruction and tampering. A record retention schedule shall be drawn up identifying essential record types and the period of time for which the records need to be retained depending upon the statutory, regulatory or contractual requirements.
- Sensitive and personally identifiable information (PII) should be sorted for a minimum duration as per mentioned retention periods and business requirements. There should be a process to securely delete data when no longer needed.
- The print records shall be stored in a separate facility adequately protected by physical security and from environmental hazards. Adequate precautions shall be taken for magnetic storage media, technology obsolescence and recovery of data related issues.

### 18.1.5. Privacy and Protection of Personally Identifiable Information

- CodeGen possesses (hosted through servers) data pertaining to its clients (associated business units), customers and its employees. Technical and organizational measures like logical access controls, non-disclosure agreements shall be implemented to protect this information and employees' personal information.

**Use of Personnel Information**

- Personal identifiable information shall only be collected and used for business purposes, and in line with relevant legislations, regulations and contractual clauses.
- Personal information shall not be shared without due consent of the concerned individual or the approval of the HR department, except where CodeGen may be obligated to share such information with law-enforcement, government and regulatory authorities, or to prevent imminent loss or harm to the concerned individual or others.
- Communications that may include personal or private information such as email, phone calls and faxes, made through CodeGen systems and networks, shall only be recorded and monitored in accordance with defined instructions, approval and after informing the concerned individuals.

**Prevention of Misuse of Information Processing Facilities**

- CodeGen's information processing facilities shall be used for business purposes only. Appropriate controls shall be implemented for preventing the usage of these facilities for non-business or unauthorized purposes. A disciplinary process shall be initiated for the inappropriate usage of CodeGen information processing facilities.

- At the time of login, a warning message shall be displayed on the computer screen indicating that the system being entered belongs to CodeGen and that unauthorized access is not permitted.

#### 18.1.6. Regulation of cryptographic controls

- Applicable rules, regulations, relevant agreements, laws shall be complied while using cryptographic keys within CodeGen. Legal advice shall be obtained wherever required to meet these requirements.

### 18.2. Information Security Reviews

#### 18.2.1. Independent Review of Information Security

- CodeGen approach to managing information security and its implementation shall be independently reviewed annually as per the CodeGen ISMS internal audit procedure, or when significant changes to the security implementation occur.
- Such reviews shall be carried out by an internal/ external resource (ISMS Auditor) that shall, at all times, remain independent from implementation of the information security controls.
- The results of independent reviews shall be recorded and reported to the ISSC.

#### 18.2.2. Compliance with Security Policies and Standards

- ISSC shall regularly review the compliance of security policies, procedures and guidelines. ISSC in its periodic reviews shall consider:
    - Causes of Non-Compliance
    - Actions to prevent re-occurrence of Non Compliance
    - Review of Corrective Actions
- Implementation team shall maintain a record of all the corrective actions. These actions shall be reviewed with specialists and internal / external auditors for improvement in security.

#### 18.2.3. Technical Compliance Review

- Only the skilled professionals shall carry out vulnerability assessments and penetration testing as part of technical compliance checking.
- Technical compliance checking shall be undertaken annually and shall cover:
    - Hardware Controls
    - Software Controls
    - Physical Security
- Utmost care shall be taken when tools are used for technical compliance checking to avoid disruption to business processes.

## 19. Latest Version of This Document

You can obtain the latest version of this document from the ISM upon approval from the CISO.

## 20. Key Roles & Responsibility

The owner of these policies is the CISO. CISO, ISM and ISSC are responsible for maintenance and accuracy of these policies.

- Should contact the Information Security Manager for any clarification of this document.