Ciel

Beyond Horizons

INFORMATION TECHNOLOGY (IT)

POLICY

Document Control

Document Distribution and Accessibility

The document shall be made available to all the staff and service providers to whom the policies relate. The document should be approved annually by the Board and a copy shall be posted on the intranet.

Revision tracker

Date	Version No.	Sections modified	Author	Reasons for modification

Annual validation tracker

Date	Version No.	Validated by	Designation

Authorisation for distribution – Approved by the Board of Directors of CIEL Limited on 29 June 2018.

Approved by:	Jean-Pierre Dalais	Jérôme De Chasteauneuf
Designation: :	Director/Group Chief Executive	Group Finance Director.
Signature: :		

Contents

Introduction

CIEL Limited is a leading diversified investment company in Mauritius, operating five business clusters spread across Mauritius, Africa and Asia. It is the parent holding company of the CIEL group of companies and is listed on the official Market of the Stock Exchange of Mauritius.

Scope

The present IT policy pertains to the following entities of CIEL Limited (thereafter referred to as "CIEL") and which are hosted on CCS Infrastructure:

- (CIEL Corporate ServicesLimited
- CIEL Finance Limited
- KIBO Captital Partners Ltd
- AZUR Financial Services Limited
- MITCO Corporate Services Ltd
- MITCO GROUP LTD
- MITCO SERVICES LTD
- MITCO Fund Services Ltd
- MITCO INTERNATIONAL HOLDINGS LTD
- CIEL Healthcare Limited
- CIEL Properties Limited

Compliance

Where specifically required, an entity may adapt this policy to its specific context and operations, however, all the minimum guidelines detailed in the present document should be abided to. If an individual violates the provisions in the policy, either by negligence or intent, CIEL reserves the right to take appropriate measures such as disciplinary actions, dismissal, legal prosecution, claims for compensatory damages, or other.

The reader should keep in mind that this entire policy relates only to the subject of information technology.

Exceptions

Any exceptions to this policy must be approved by the CEO or Head of Finance. All exceptions to policies shall be formally recorded, tracked, and reviewed.

Applicability

This IT policy applies to all information assets and processes. It also applies to all personnel, outside consultants, contractors, temporaries, clients or third parties accessing CIEL information assets.Employees and other individuals who gain access to CIEL information shall be bound by a duty of confidentiality which shall endure indefinitely.

1 Strategic

1.1. IT Strategy and Budgeting policy

1.1.1. Objectives

This policy establishes guidelines to ensure that all IT related decisions are in line with CIEL's business strategy.

1.1.2. General Guidelines

- The IT strategy should be consistent within the Group and be aligned to the organisational goals.
- The IT strategy should be formally approved by the Board of Directors.
- The IT strategy should be focused upon mitigating IT and non-IT risks.
- The IT strategy should be reviewed on an annual basis.
- The implementation of the IT strategy should be within the predetermined time frame established by the Board.
- The IT Administrator should make sure that the IT strategy adapts to the changes of the business requirements.
- The IT strategy policy should specifically cater for:
  - Present and future needs concerning hardware, software and networking architecture.
  - All standards and strategies in terms of acquisition, in-house development, outsourcing and management of hardware and software solutions.
- The IT Administrator should ensure that the IT strategy is in line with the revenue, profitability and competitive advantage of CIEL.
- The IT strategy should maximise efficiency by emphasising on using standardised processes, being up to date with technological advancements and saving time through the use of technology.
- The IT Administrator should prepare an IT Budget yearly, ensure that it is in line with the entity's strategy and budget and take the following into consideration during its preparation:
  - Capital expenditure forecast for hardware and software
  - Maintenance forecast for hardware and software
  - Other IT Costs to be incurred to achieve objectives set in the IT Strategy
  - New/ongoing projects.
- The IT budget for each entity should be validated by the Head of Finance.
- The IT Administrator should ensure that the IT budget and strategy considers both current and future IT projects by being responsive to changes in the business

environment. Any variance from the IT budget should be justifiable and appropriate corrective actions taken.

- Discrepancies from the IT budget should be reasonable and corrective actions should be taken.

2. Security of Information Systems

2.1. Logical and user access control policy

2.1.1. Objectives

The objective of this policy is to ensure that only authorised persons have access to the IT systems of each entity and that only authorised functions are performed. The guidelines provided in this policy are applicable at application, operating systems and database level. Access to all information resources should be granted in a very controlled manner and be solely driven by business requirements. This policy applies to all types of IT systems of the infrastructure such as the domain controller (Windows Active Directory servers), business applications and network folders hosting business files.

2.1.2. User access management

- All user access should be driven by specific business requirements. The user access requirements should be profiled based upon job description, responsibilities, or function. The use of profiles assists in management of user access, and provides consistency. The definition of the access rights to be granted should also take into consideration the avoidance of any conflict in segregation of duties of the user within the day to day responsibilities allocated to him or her.
- Access rights should be granted to users based on a detailed user rights matrix whereby each user's job profile is mapped onto the required access rights to applications. The user rights matrix for each application/ system should contain at a minimum the following:
  - o The functionalities available in each application
  - o The minimum access rights required by each profile
  - o The user accounts linked to each profile
- Instances where segregation of duties is not possible should be documented and approved by the data/system owner.
- Incompatible tasks performed by the same person should be reviewed at least annually by the respective Head of Department.
- Any special privileges granted to users on technical platforms (e.g., administration accounts for operating systems, databases or applications, or accounts that can override system or application controls) should be based upon function and job requirements. These privileges should only be allocated on a "need-to-have" basis for technical support or operations processes.

- Remote (Virtual Private Network) and privileged access to the network domain should be managed exclusively by the IT Administrator. Refer to remote access policy detailed guidelines on this subject.

2.1.3. Granting of access to IT applications

- Access to any IT application should be granted only after formal approval by the relevant Head of Department.
- Access to each IT application should be managed by means of a unique user ID/code and password combination.
- Use of generic IDs should be restricted as far as possible and should only be allowed for necessary business or operational reasons. Use of generic IDs should be formally documented and approved. Additionally, generic IDs should be used on a temporary basis only and be deactivated immediately if no longer in use.
- Access to operating systems and databases should be controlled at these levels by the IT Administrator and should not be granted to business users.
- Temporary access if required should be revoked on a timely basis. Automatic termination of temporary access should be enforced where possible.
- No access should be granted by IT Administrator without a formalised business request.

2.1.4. Modification of user access rights on IT applications

- All requests for modification of access rights should be supported by the business reasons and approved by the Head of Department.
- Approved requests should be forwarded to the IT Administrator so that the rights can be modified.
- No access should be modified by the IT Administrator without a formal business request.

2.1.5. Revocation of user access

- Any employee departure or transfer should be communicated to the IT Administrator immediately by the Human Resource (HR) department requesting that all access be revoked.
- The IT Administrator should immediately revoke all user accounts on all IT systems upon receipt of the request and inform the HR Department and the Head of Department.

2.1.6. Segregation of duties within the user access management process

- Segregation of duties within the user access management process should be observed at all times for the following:
  - Request for user account creation
  - Approval of request
  - Modification of user accounts
  - Account activity monitoring

2.1.7. Periodic review of user access rights

- All user access rights on each IT application should be reviewed by the relevant Head of Department once a year to ensure that user access rights remain commensurate with their responsibilities.
- The periodic review should be conducted as follows:
  - On a frequency defined by CIEL, the IT Administrator extracts all users and access rights on all the business applications, and the accounts on the Windows Domain.
  - The list is communicated to the relevant Head of Departments for validation.
  - The Head of Departments review the lists received above, indicate any amendment if required, and send back the updated list (dated and signed) to the IT Administrator. In the event that no change in rights is required, the Head of Departments formally reconfirm the appropriateness of the access rights granted to their staff.
  - The IT Administrator makes the changes to each user account as per the reviewed list of access rights.
  - The IT Administrator should retain all the signed forms.

2.1.8. Management of administrative/privileged access

- Administrative/privileged access provides the grantee unlimited privileges on IT systems. Administrative/privilege access should be restricted to the IT Administrator and designated service providers only.
- Individuals having administrative/privileged accounts should use a separate, non-privileged account for performing non administrative functions.
- All activities of privileged users should be monitored by an independent party on a regular basis. Additionally, privileged users should not be given monitoring functions.
- All privileged accounts should be reviewed by an independent personnel (e.g. a security officer) at least yearly to ensure that they are still commensurate to the user's duties.

2.1.9. Review of critical activities

- Critical activities on business applications should be identified for all entities.
- Heads of Departments together with the IT Administrator should define which critical activities should be monitored and logged and the frequency of review. Impact of transaction logging on performance of IT resources should be assessed so as not to cause business disruptions.
- The IT Administrator should ensure that all activities monitored are approved and communicated to the relevant Heads of Departments.
- Access to monitoring logs should be restricted to protect them from unauthorised access or tampering.

- The logs should be kept as required by relevant physical security requirements. In case of investigation, all logs should be retained till resolution of the incident.
- End users should be informed by the IT Administrator that their use of corporate or personal IT infrastructure, services, systems and applications may be monitored by authorised personnel as permitted by this policy. ;

2.2. Password policy

2.2.1. Objectives

The objective of the password policy will ensure that access to information systems will be granted only to authorised users through the use of a password. The policy also provides guidelines for management of passwords and their protection.

2.2.2. Password management

- Access to devices and information should be controlled through the use of passwords.
- The IT Administrator should configure the password settings on each IT system according to the guidelines given below in 2.2.6.

2.2.3. Password protection

- Passwords to system users should be communicated in a secure manner and unprotected medium of communication should be avoided; for instance the use of unprotected electronic mail messages.
- Passwords should be mandatorily changed upon first log-on.
- Passwords should not be stored on computer systems (e.g. excel sheets) or any other unprotected media. Instead, password for critical systems should be placed in a sealed envelope and kept in a safe which is restricted to the Head of Finance and the IT Administrator.
- After the installation of systems or software, default vendor passwords should be changed.

2.2.4. Password reset

- Requests for password resets should be formally done by mail to the IT Administrator providing reasons for the resetting of password.
- The IT Administrator should perform the password reset and keep a log of all password resets.
- All passwords which have been reset should be changed upon first log-on by the user.

2.2.5. User responsibility

- Password should be kept confidential.
- Keeping record of password (e.g. paper, post its, software file or hand-held device) should be avoided.
- Change of password should be done every 90 days and the re-using of old passwords should be avoided.

- Quality passwords with sufficient minimum length should be used.
- Passwords should be changed at first log-on the user
- The same password should not be used for business and personal purposes.
- The "Remember Password" feature of application programs must never be used.

2.2.6. Password requirements for user accounts

- The minimum length of a password should be 7 characters and at least 3 of the following four types of characters should be used:
  - Lowercase
  - Uppercase
  - Numbers
  - Alphanumeric characters
- The passwords can never be reused.
- The maximum password age should be 60 days.
- The minimum password age should be 1 day.
- After 5 failed attempts, the user account should be locked.
- The idle session timeout should automatically activate after a maximum of 10 minutes.
- Passwords should not be stored using reversible encryption.

2.2.7. Privileged account passwords for privileged/administrative accounts

- Passwords for privileged accounts should be differing across all systems.
- Minimum length should be 10 characters.
- Passwords should have minimum complexity; dictionary words should not be used. Passwords should use at least three of the following four types of characters:
  - Lowercase
  - Uppercase
  - Numbers
  - Alphanumeric characters
- The passwords can never be reused.
- Maximum password age should be 60 days.
- Minimum password age should be 1 day.
- After 3 failed attempts, the user account should be locked.
- Locked passwords for privileged accounts should be manually unlocked by Administrators.
- The idle session timeout should automatically activate after a maximum of 10 minutes.
- Passwords should not be stored using reversible encryption.
- All setting should be validated by CIEL.

2.3. Antivirus policy

2.3.1. Objectives

This policy will provide the organisation relevant guidelines to ensure the protection of the company's data against malicious software such as viruses, spyware and other forms of malware that could negatively impact on the confidentiality, integrity and the availability of electronic information.

2.3.2. General guidelines

- Effective anti-virus software should be used and maintained up-to-date on all servers, workstations and devices.
- Anti-virus software upgrades should be made available from the IT Administrator as soon as they are received from the supplier.
- The IT Administrator should make sure that the virus protection software does not have a significant and negative impact on the system performance.
- Provision to protect devices not connected to the centrally maintained anti-virus should be made by the IT Administrator.
- Automatic scan of removal media for presence of malware should be performed.
- Only the IT Administrator should have access to amend anti-virus software configuration.
- Employees should immediately report to the IT Administrator on any virus outbreak so that appropriate actions can be implemented.
- Upon the identification of a malware, any infected device should be immediately disconnected from the network until the virus has been cleared and until the anti-virus software has been updated so as to prevent the spread of the virus.
- Any client device which is connected to the network should have an updated antivirus.

2.3.3. Best practices for Virus Prevention

- Files, attachments and links received from unknown and suspicious sources should not be opened.
- Any e-mail messages containing links to unknown web sites should be treated as untrustworthy and should not be opened.
- Any request for the installation of software should be made to the IT Administrator through the helpdesk system.
- To avoid the sharing of storage media with read/write access.
- Regular backup of critical data on the file server.

2.4. Intranet and Internet policy

2.4.1. Objectives

The objective of this policy is to make sure that the internet and intranet access facilities through the network are adequately used and to make the users abide by the acceptable use policy.

2.4.2. General guidelines for the intranet

- In the event that CIEL decides to set up an intranet, all data present on the intranet should have a designated owner.
- The IT Administrator should ensure that adequate security permissions are assigned to the folders on the Intranet so that users only access information which pertains to their functions.
- Since information contained in the intranet is confidential, users should not share or divulge any documents to third parties outside the organisation.

2.4.3. General guidelines for internet

- The IT Administrator should determine, consent to and keep record of a list of content categories that the employees are allowed to access.
- The IT Administrator should establish appropriate security mechanisms to control access to websites that are defined as unacceptable as defined by the IT Administrator.
- Sensitive information communicated over external network should be encrypted.
- The IT Administrator in collaboration with other concerned department should organise trainings on a yearly basis to educate employees upon the Internet usage policy.
- The IT Administrator should crosscheck the internet activities of the employees and escalate and report any violations.
- Access points should also be well defined in the policy, and needs to be classified into segments from CIEL's internal wired LAN through the use of a firewall so as to distinguish among networks.
- The access point console should be protected by a password which complies with CIEL's Logical and User access control Policy and password Policy.
- Protocols which are not compliant with security policies concerning the access points should be disabled, for example; threshold parameters concerning WIFI and inactive time frames.

2.4.4. Acceptable use of the internet

- Connections from CIEL's network to the Internet should be made through a browser approved by CIEL.
- Internet access should be strictly for professional use, unless permission has been granted by the relevant Head of Department.
- Files should not be downloaded wherever possible, otherwise, all downloaded files from the internet should be scanned for viruses being in line with the antivirus policy.
- Employees may download and install any software on the company owned device, as long as approval has been granted by the IT Administrator and the relevant Head of Department.

2.4.5. Prohibited activities

- CIEL's Internet/Intranet cannot be used to send, document or store any material classified as any of the following;

  - Offensive
  - Vulgar
  - Harassing
  - Disrespectful
  - Pornographic
  - Derogatory
  - Racially prejudicial
  - Defamatory
  - Anything which is likely to involve CIEL in any civil or criminal litigation
  - Any material breaching any copyright or intellectual property rights
  - Creating any forged instrument
- The entity shall not be liable for any material downloaded or depicted by employees on any public communications network. If there is any breach or violation, the employee will be held responsible.
- All information downloaded should be scanned and used strictly for business purposes unless these are approved by the IT Administrator and the relevant Head of Department.
- Users should not download any executables unless these are approved by the IT Administrator and the relevant Head of Department.

2.4.6. General security guidelines

- The IT Administrator should configure the security settings in the approved web browser.
- The right of amending any security setting should be restricted to only the IT Administrator.
- The IT Administrator should install and maintain any firewall and other detection devices.

2.4.7. Making network connections

- Only trusted entities are allowed full access to CIEL's network. All entry points to the CIEL's network must be reviewed and approved by the IT Administrator.
- Any connections made should not incur a degradation of security to CIEL's network.
- All connections with external networks should be approved by the IT Administrator.
- Prior to accessing CIEL's network, all third party should ensure that they are secured in a manner consistent to CIEL's requirements.
- If required, computers or networks may only be connected to third party computers or networks after the IT Administrator determined that the combined system will be in compliance with CIEL's security requirements.

- All connections between CIEL's internal networks and the Internet (or any other publicly-accessible computer networks) must include an approved firewall and related access controls. A business justification signed by the CEO or Head of Finance and application proxy service via an approved firewall are required.

2.4.8. Control of network connections

- All CIEL's internal network addresses including configurations should be strictly confidential.
- Any changes made to the network which could significantly affect CIEL's network security should be formally approved by the CEO.
- The IT Administrator should maintain a register which covers all categories of connectivity to into or from CIEL's network including remote access, private, internet administration and maintenance, internet service usage...
- All connections between CIEL's and external networks are required to use approved security technology and procedures.
- The number of connections between CIEL and public networks should be kept to a minimum.
- Secure gateways, firewalls, and other protection devices should be used to maintain the level of security when elements of different trust levels are brought together.
- Security systems operating within and across public and CIEL's networks should be protected against internal and external intruders. The systems are to be installed in a physically secured and access-restricted area.

2.4.9. Monitoring of network activity

- Internet activity on the network should be monitored on a monthly basis.
- CIEL should make use of a firewall together with an Intrusion Detection System to restrict incoming and outgoing traffic to ensure that unauthorised connections are not made.
- All unused ports should be closed to prevent unauthorised connections
- Firewall rules should be reviewed quarterly by the IT Administrator and communicated to CIEL management.

2.5. Remote Access policy

2.5.1. Objectives

The objective of this policy is to establish the guidelines for connecting to the company's network from any external host.

2.5.2. General guidelines

- Use a two-factor authentication for remote connections to CIEL internal network and emails.
- The IT Administrator should be responsible for granting and revoking remote access to the IT resources.

- Contracted support personnel will be provided with remote access to the network only if they need to use that particular utility for their work purpose. The access should be open only during the period required.
- The IT Administrator needs to ensure that remote access is controlled through a password.
- The IT Administrator should monitor remote access and track any unsuccessful attempts.
- All IT security breaches should be immediately escalated to management
- The IT Administrator should verify that the remote user's computing devices abide by the security requirements.
- Remote access to the specific systems and networks need to be confined to the use of only authorised persons and be subjected to review so as to avert unlawful access. These can be enforced by implementing a system which requires accountability which eventually can lead to traceability.
- If VPN is used;
  - The IT Administrator should ensure that VPN server is properly functioning.
  - Access should be granted by the IT Administrator and should be reviewed annually.

2.6. Email usage policy

- Email should be used primarily for legitimate business purposes in the course of assigned duties. Any personal use should not interfere with these duties or compromise the security or the business and may only be incidental and occasional in use.
- Chain email messages which are not business related should not be forwarded.
- It is strictly prohibited to disclose CIEL employees' or third party contractors' emails for mass mailing purposes. It is prohibited to send bulk mails of personal nature without prior approval.
- CIEL considers that all messages circulated through the organisation's email system is CIEL's property. The IT Administrator can monitor any employee's email without prior notification provided that the monitoring is done in accordance with the provisions of the law. Thereby, CIEL has the right to take any necessary disciplinary action which might lead to the termination or even entail litigations if the employee is not abiding by the pre-set guidelines.
- Employees should be accustomed to the maximum email attachment size:
  - Incoming email size: 50MB maximum
  - Outgoing email size: 50MB maximum
- Employees should refrain from sending confidential information by email. If needed urgently the email should be protected by a password and should be communicated to the recipient but not through an email but rather another means of communication.
- Employees have the responsibility to conduct backups of their archive email folders.

- Employees are highly encouraged to tidy up their mailboxes and to delete or archive emails which are judged as no longer needed.
- Employees should refrain from forwarding emails to and from external addresses.
- CIEL should include a disclaimer in all the emails being sent which will cover breaches of confidentiality, propagation of viruses, contractual claims and employee liability.

2.6.1. Personal Use

- CIEL's email system is only for business purpose, nevertheless CIEL allows for occasional personal use of emails given that the employee abides by the following conditions:
  - Personal use of any emails should not cause any hindrance to the employee's work.
  - Employees who access their personal mail through CIEL's assets should abide by the password, Internet/Intranet, and Antivirus policies.

2.7. Social Media

- The IT Administrator has the responsibility to manage access to social media through the organisations' device, appropriate filtering should be applied whenever required.
- If an employee needs to access social media, his/her request should be approved formally by the head of department and then forwarded to the IT administrator to actually give the access.
- Only authorised staff from the communication Department is granted access to post information on social media concerning CIEL.
- CIEL permits the usage of social media for personal purposes if the following conditions are met:
  - Employees are personally responsible for any content they upload or post on social media.
  - Employees should read and comply with the terms and conditions of the social media platform which they are using.
  - Employees should not upload, forward or post any material which belongs to a third party without the consent of the third party.
  - Employees should not upload, post, forward or post any content which relates to section "3.3.5 Prohibited activities" of the internet and intranet policy.
  - Employees should not upload, post or forward any content belonging to a third party unless upon the consent of the third party.
- Employees should use the following disclaimer if they want to publish materials related to their work: "The postings on this site are my own and don't necessarily represent those of CIEL. I remain solely liable for my publication".

- Employees are prohibited to conduct any business with any customer via any social media channel.
- Employees should be conscious that any misuse of social media may give rise to potential litigations.
- Employees who feel hassled or bullied, or offended by any material uploaded or posted on any social media channel are encouraged to voice out their grievance to the HR Department.

2.8. Software Whitelist

2.8.1. Objectives

This policy specifies the software which have been approved by CIEL.

2.8.2. General guidelines

- The IT Administrator should perform monthly monitoring of all user machines to check if these types of software are installed
- Users found with prohibited software on their machines will be subject to disciplinary actions.
- Illegal "pirated" or "bootlegged" copies of software or data are not permitted on CIEL's networks. Some examples are evaluation copies in production environment, no license, or number of licenses exceeded.
- Programs that are designed to investigate and/or exploit CIEL's information security environment (including password crackers, scanners, network sniffing devices, network packet sniffing devices and other "hacking" tools) are prohibited, except when expressly authorised by the IT Administrator.
- It is strictly prohibited to download software on any CIEL devices from the internet where proper licensing requirements are not provided, except when it is authorised by the IT Administrator.
- Only upon approval from the IT Administrator may personal software be installed on CIEL's equipment. CIEL therefore reserves the right to access and/or remove such software when there is neither reasonable justification nor approval for such installations.

2.8.3. List of permitted software

Refer to Appendix B for the list of allowed software by CIEL.

2.8.4. List of blocked websites

Refer to Appendix C for a list of websites blocked by CIEL.

2.9. Cloud security guidelines

- CIEL should ensure that a contractual agreement exists with the cloud service provider whereby the latter engages itself to protect all CIEL's confidential data.
- CIEL should ensure that the following are catered for by the cloud service provider:

- CIEL's data should be encrypted while transiting networks.
- CIEL's data and devices storing the data should be protected from any tampering or loss.
- There should be separation of data between other customers, to avoid compromising confidential data.
- The service provider should abide by a governance framework which needs to be aligned with that of CIEL.
- The service provider should have a contingency plan to deal with operational security.
- The cloud service provider should conduct proper screening before recruiting any personnel.
- The service provider should provide CIEL with services that mitigate risks to the latter's security.
- The cloud service provider should ensure that the services being provided meets the expectations and requirements of CIEL.

3. User awareness

3.1. Objectives

The purpose of this policy is to provide guidelines concerning the awareness and buy-in of users, including external service providers, to the policies.

3.2. User awareness and engagement policy

- Acknowledgement of user related IT policies should be obtained via signature and retained in the employee's file by the HR Department.
- External service providers who have access to CIEL's IT systems should be provided with the policies applicable to the services rendered, and acknowledgement should be formally obtained via signature and retained at CIEL
- IT security awareness policies should be implemented and enforced so as to promote good practice among all users of the IT systems.

3.3. User awareness and communication strategy

- All policies should be communicated to the related users after their approval.
- Final approved versions of policies should be made available to the end user on a central repository or the intranet.
- The IT department should organise trainings in order to refresh employees about the IT security guidelines on a yearly basis.
- In the event of revisions to the policies, these should be immediately communicated to the end users so that same can be implemented.
- The IT Administrator should regularly communicate to the users about the specific threats or new threats which can significantly impact them.

4. Software update

4.1. Objectives

The objective of this policy is to establish a process that defines how updates are carried out for either servers or workstations, and specifying who is responsible to perform the updates. This is to ensure that all IT systems are up-to-date and are equipped with the latest security patches.

4.2. Software and Operating System Update policy

- The IT Administrator should make sure that regular checks are conducted and that appropriate clean ups upon the system is performed.
- The IT Administrator should conduct regular monitoring to ensure that all updates have been properly performed.
- Backup, virus detections and programme installations should be monitored and should be in line with the other policies.
- Software upgrades should also be monitored to ensure efficiency and effectiveness of the IT infrastructure.

5. Incident Management

5.1. Objectives

This policy will provide a framework to handle IT disruptive events and information security incidents that can have an impact on business operation, IT dependent operations, regulatory compliance, financial position, intellectual capital and technology resources.

The policy will ensure that the incidents are treated taking into account their relative priorities with a view to reduce its adverse effect on the organisation.

For any incident which occurred, a thorough analysis should be conducted to recognise the cause and to implement preventive measures.

5.2. General guidelines

- Identification and reporting of incidents

Employees, contractors and third parties should quickly respond to the occurring of any incident and immediately report to the IT Administrator. There should be a dedicated helpdesk or a staff in charge of recording and prioritising the incidents. The helpdesk staff should then communicate all the incidents to the IT Administrator.

The IT Administrator is also responsible for the tracking of any potential incidents which may occur and regularly report to management level.

- Analysis and Categorisation of Incidents

Incidents should be prioritised based on its impact and urgency so as to identify the time required for actions to be taken.

Incident impact: measures the potential damage caused by the incident on business operations.

Incident urgency: measures how quickly a resolution of the incident is required.

A table for the categorisation of the incident urgency and the incident impact can be used in order to class the incident priority.

Category of incident impact	Description
High (H)	▪ The incident affects a large number of staff preventing them from performing their normal business activities ▪ A large number of users are affected. ▪ The incident highly damages the reputation of the business.
Medium (M)	▪ The IT incident prevents a moderate number of staff to do their job properly. ▪ A moderate number of users are affected. ▪ The damage to the reputation of the organisation is likely to be moderate
Low (L)	▪ The incident does not critically affect the organisation and the number of staff affected is minimal. ▪ Very few users are inconvenienced. ▪ Minimal damage to the reputation of the organisation.

Category of incident urgency	**Description**
High (H)	▪ The damage caused keeps on increasing. ▪ Work that cannot be done by employees is time consuming. ▪ A large number of users are affected.
Medium (M)	▪ The damage caused increases at a moderate rate. ▪ A single user or very few users are affected.
Low (L)	▪ The damage caused increases at a slow pace. ▪ The work that cannot be completed by staff is not time sensitive.

Based on the incident impact and the incident urgency, an **Incident Priority Matrix** can be used to measure how quickly should the incident be resolved:

		Impact		
		H	M	L
Urgency	H	1	2	3
	M	2	3	4
	L	3	4	5

Priority Code	**Description**	**Target Response Time**	**Target Resolution Time**
1	Critical	Immediate	1 Hour
2	High	10 Minutes	4 Hours
3	Medium	1 Hour	8 Hours
4	Low	4 hours	24 Hours
5	Very Low	1 Day	1 Week

- Monitoring and Post-event Analysis of Incidents

  The IT Administrator needs to monitor the status of the reported incidents and the incidents which have not been treated in the targeted resolution time should be investigated if necessary.

  The IT incidents need to be well documented to allow subsequent analysis and to initiate corrective actions with a view to prevent similar incidents to recur.

  Below are actions to be taken by the IT Administrator:

  - Update existing IT security measures for the resolution of incidents.
  - Introduce new measures so as to prevent the incident to recur, for example; forcing changes of passwords or modify the accounts of workers who are directly involved or affected with the incident.
  - Recurring incidents should be analysed to determine the root cause.
  - Take disciplinary and corrective actions against those responsible for the incidents.

6. IT Operations

6.1. IT Asset Management policy

6.1.1.Objectives

The objective of this policy is to provide guidelines for the management of assets in a consistent manner in order to ensure that the assets are being efficiently used, secured and tracked for any financial reporting, resource optimisation and business continuity purposes.

Note: The term "asset" include all elements of software and hardware that are found in CIEL's business environment.

6.1.2.Ownership and inventory

- All assets under the property of CIEL as well as personal devices brought for business purposes should abide by the rules of the end user policy. Users of smartphones and tablets should also abide to the IT policy.
- A custodian must be assigned for maintaining and securing the assets. The custodian does not have any property rights to the asset but he may delegate his tasks to other individuals.
- A full-time custodian (in general the Head of Department) must be assigned for assets used by a part-time personnel.
- The IT Administrator should set-up and maintain an IT Asset Inventory Register which will record the following minimum information for each assets: serial number, description of the asset, location and the custodian.
- Additional information for ease of reference for each asset may be maintained. The additional illustrative details may include where relevant: memory capacity,

purchase price, warranty period, insurance cover, license and years until replacement.

- The IT Asset Inventory Register should reflect any records maintained by the other departments for financial or operational purposes.

6.1.3. Tracking and Monitoring

- The IT Administrator should ensure that all assets are easily identifiable.
- Vendor decals, stickers and other serial identifiers should be kept and recorded for tracking purposes.
- All the IT assets that are not connected to the network for more than one month should be identified and the IT Administrator should ensure that they are still in operation in the assigned department.
- Surprise audits should be performed on a sample of selected assets that are not connected to the network with a view to ensure that the assets are still in operation in their assigned department.
- A monitoring exercise should be conducted at least once every year by the IT Administrator in order to determine whether the IT Asset Inventory Register is accurate and complete.
- Findings on any inconsistencies during the monitoring exercises of the IT Asset Inventory Register should be analysed, updated where relevant and communicated to the Head of Finance.
- Any assets, which cannot be located should be reported to the relevant custodian and the Head of Department.

6.1.4. Asset Management

- Assets purchased should be recorded in the IT Asset Inventory Register before allocation and use.
- It is the responsibility of the custodians to notify the IT Administrator about unneeded assets so that these can be re-allocated for other business needs.
- Without any written authorisation, assets cannot be removed from the premises by end-users which includes employees and contractors. Exceptions can be made for the following: mobile/smart phones, tablets, laptops and portable devices.
- Any assets removed from the company premises are under the relevant custodians' responsibility and should be kept physically secure according to their monetary value.
- The asset custodians are held responsible to notify the IT Administrator of any movement or reallocation of assets so that the IT Asset Inventory Register can be updated accordingly.
- It is the responsibility of the asset custodians to notify the loss or theft of any assigned assets to the Head of Department and the IT Administrator within 24 hours upon the detection of the incident. Refer to the IT Incident Management Policy for detailed guidelines.

- Damaged assets should be notified to the IT Administrator by the asset custodians so that appropriate actions in consultation with the relevant Head of Department can be taken based on the cause of the damages.
- The custodians of shared physically moveable assets that are used by other parties should ensure that the use of the equipment by the different parties is recorded and signed off upon the issue and the return of the asset to the custodian; for instance projectors.
- Assets that have reached the end of their useful life should be disposed as per the IT Asset Disposal Policy.

6.2. IT Asset Disposal policy

6.2.1. Objectives

The objective of this policy is to define consistent standards for the retirement or disposal of IT assets with a view to prevent loss of information, maintaining confidentiality of information and to ensure efficiency and compliance with applicable regulations.

This policy is applicable for all tangible IT assets which include hardware for instance desktop equipment, communications equipment or removable media.

6.2.2. Asset identification

- Reasons for retirement or disposal of assets include obsolescence, failure or the equipment having reached its end of useful life.
- Assets which need to be retired or disposed of should be identified by the IT Administrator.
- The residual value of assets identified should be determined by the Head of Finance.
- The IT Administrator should consult with the Head of Finance in order to determine the approach to be used with the following options:
  - Retirement: Re-sale of the asset or donation
  - Disposal: Re-use of specific parts, recycling or physical destruction.
- After the approach has been agreed, this should be documented on the IT Asset Disposal Form.

6.2.3. Storage

- The IT Administrator should store the assets identified for either retirement or disposal, in a designated location.
- The access to the storage locations should be restricted only to authorised personnel which will include the IT Administrator and the Risk Manager.
- Assets selected for disposal should be kept for a maximum period of one year. If assets selected for retirement remains in storage for more than one year, it should be disposed.

6.2.4. Retirement or disposal

- The IT Administrator is responsible to erase all data prior to the asset to be disposed or retired.
- The status of the assets earmarked for retirement or disposal should be updated by the IT Administrator in the IT Asset Inventory Register.
- In the event of retirement or disposal of assets, the IT Administrator should to assess the contents of media devices and perform a backup of business critical information for future references.
- The IT Administrator should ensure that the software licences on the retired or disposed assets are reclaimed and re-used.
- If a third party is considered for the recycling or physical destruction of assets, contractual obligations should be formalised and a non-disclosure agreement signed by the third-party.
- If the assets have been designated for re-sale or donations, a letter should be signed by the recipient absolving the company from any potential legal responsibility. The letter should contain the following clause which has been vetted by the CIEL's Corporate Legal Department:

  "I hereby acknowledge that the equipment bought [or donated] from the Company can have defects. I am therefore aware that CIEL shall bear no responsibility or liability of any kind pertaining to that sale [or donation], and I therefore undertake to indemnify the Company against any loss, liability and costs incurred by CIEL as a result of any actual proceeding, claim or other legal recourse brought by me, or the company on behalf of which the equipment described hereunder was bought [or donated]."

- The IT Administrator and the Risk Manager should ensure that the methods used for the disposal of assets are environment friendly.

6.2.5. Sanitisation of Media Devices

- All media devices should be purged before disposal. The IT Administrator should ensure that adequate sanitisation procedures are performed for both the retirement and disposal of media device (including hard disks).
- General methods commonly used for sanitisation are as follows:
  - Clear: The use of software or hardware products to overwrite the user-addressable storage space on the device.
  - Purge: The use of a non-standard means to protect confidentiality of information against laboratory attack. Executing the secure erase firmware command on a disk drive and degaussing are acceptable methods of purging.
  - Destroy: The actual physical destruction of the storage device to ensure the subsequent inability to use the media for storage of data or to recover information.

6.3. IS Acquisition Management policy

6.3.1. Objectives

The objective of this policy is to monitor the process for acquisition, implementation and maintenance of new information systems, so as to mitigate any adverse risk it may have on the business process

6.3.2. Business Requirements Specifications

- Requirements specifications should be focused upon the user needs, its performance, reliability and security requirements.
- The requirements specifications should first be approved by the IT Administrator before proceeding for proposal requests from vendors.
- There should be close collaboration with business users when determining requirements specifications to ensure that the information systems meet their specific requirements.

6.3.3. Implementation

- The IT Administrator should ensure segregation of IT environments (development, testing and production).
- Testing of the information systems should be recorded and should be signed off by the end-users if the Information system has passed the user acceptance policy conducted in specific test environments.
- Rollback plans should be considered when shifting the information systems into live environments.

6.3.4. Licensing

- The IT Administrator should make sure that any software installed on any company owned hardware by third parties hold a valid license.
- The IT Administrator should maintain a log book where all software licenses are recorded and reported regularly to the management. The logbook should contain the date that the software license was purchased and its expiry date.

6.3.5. Maintenance

- The IT Administrator should ensure that binding contracts and Service Level Agreements (SLAs) exist with the vendor of the information system upon maintenance and upgrades.

6.4. IT Procurement and Vendor Management policy

6.4.1. Objectives

The objective of this policy is to provide guidelines and specific standards for the selection of vendors and acquisition of IT resources.

6.4.2. General guidelines

- Any acquisition of IT resources should be formally requested to the IT Administrator.

- The IT Administrator and the Risk Manager should perform a risk assessment and any kind of obligations in the process of evaluating the purchase of any server.
- Any procurement of IT resources should be approved by the following specific level of authority:
  - All CAPEX IT resources should be as per the existing procurement procedure.
  - The IT Asset Inventory Register should be updated upon acquisition of IT resources.
  - All IT purchases for CCS are budgeted once per year and amount is approved by the board of CCS. Along the year all quotes are approved by The Head of Finance when they are big purchases. Approval is not required for small purchases like USB drives, mouse, keyboards etc. However, any unbudgeted item should be approved by the Head of Finance.
  - All purchases should be in line with the procurement policy or similar guideline in the absence of a formalised document.

6.4.3. Vendor Management

- For NON CAPEX IT resources (e.g. consumables) the IT Administrator should be responsible to consult potential suppliers and ensure that request for bids are reachable to them.
- The IT Administrator may request details from qualified technical personnel.
- Service Level Agreements should be described for all critical IT resources based upon the entity requirements.
- A review process should be implemented every three years, where the IT Administrator reviews the performance of the suppliers against the second next best supplier's proposal. The IT Administrator should identify and prepare for foreseeable risks concerning the supplier's ability to continue the delivery of services.
- Criteria for selection and re-evaluation of suppliers should be recorded and acceded by the IT Administrator.

6.4.4. Third party management

- All third parties appointed by CIEL should be bound by valid contractual agreements.
- Contractual agreements should clearly stipulate the level of service offered in terms of clear response times.
- CIEL should ensure that all third parties sign a confidentiality agreement in the event that they have access to sensitive organisational data.
- In the event that CIEL outsources a portion of its business activities to third party, CIEL should ensure that the latter provides a regular reporting of the work performed to the CEO/Head of Finance.
- In the event that third parties require access to CIEL's IT systems, a formal request should be made by the appropriate party and approved by the CEO.

7. Continuity Management

7.1. Backup policy

7.1.1. Objectives

The objective of this policy is to ensure that applications and data supporting business operations can be completely and accurately recovered within time frames acceptable to the business in the event of a system failure, destruction of data or disaster.

7.1.2. Scope of the backup policy

- This policy applies to the following components:
  - Hardware (all workstations and laptops, file servers and email servers)
  - Software (database and operating systems hosted on all critical servers, IT applications and all business critical application data)
- The scope excludes personal data stored on workstations, laptops and mobile devices. Refer to the End User IT Policy for requirements and guidelines relating to back up of information stored on workstations, laptops and mobile devices.

7.1.3. Backup identification

- The business users in collaboration with the IT Administrator should determine which applications/system files/databases need to be backed up.
- The IT Administrator should validate, document and maintain a backup strategy document covering all IT systems in scope. Data files/folders to be backed-up on each IT system should be formally documented and approved in the backup strategy.
- The IT Administrator should ensure that a centralised and registered backup software is used to perform the backup.
- Access to the backup utility should be restricted to the IT Administrator only.
- In the event that a section of the backup is outsourced to a third party, the IT Administrator should ensure that the latter provides a daily backup report detailing the status of the backup and any actions performed.

7.1.4. Backup schedules and frequency

- Full backups should be scheduled to run during off peak hours.
- The IT Administrator should ensure that backup is performed in line with the documented backup identification section defined as per section 7.1.3 above.
- All changes made to the backup schedules should to be approved by the IT Administrator and relevant business owners.

7.1.5. Backup monitoring and incident management

- The IT Administrator should monitor the backup status on a daily basis. In the event that the IT Administrator is unavailable, the backup status should be monitored by a designated person.

- The IT Administrator should investigate all backup failures and perform corrective actions accordingly. However, these actions should not impact the normal business operations.
- All backup logs and evidence of verification of daily backups (e.g. completed daily IT operational checklists) should be archived.

7.1.6. Backup media

- Backup media used to perform backups may include tapes, disk or other appropriate media as approved by the IT Administrator. Spare tapes should be available for replacement of non-functioning or damaged tapes.
- Tapes should be rotated wherever possible every week.
- Data backed up should be encrypted.
- All backup media should be clearly labelled to facilitate identification.

7.1.7. Backup retention

- Backup data should be retained for a period as defined below or as required by law and regulations, whichever has the longest duration.
    - Daily backup – 1 month
    - Monthly backup – 1 year
    - Yearly backup – 7 to 10 years or as required by the regulatory authority

7.1.8. Restoration of backups

- The IT Administrator should perform appropriate data restoration tests on a monthly basis to identify faulty backup media and improve the likelihood of a successful restore in the event of an incident
- Full restore testing of all backup media should be performed every year.

7.1.9. Offsite backup storage

- All backup media should be kept in secure onsite and offsite locations accessible to authorised personnel only at all times. The daily, weekly, monthly and yearly backups should be sent to the designated offsite location as defined in the backup strategy document.
- The IT Administrator should record physical backup media movements between the primary and offsite locations. A physical backup media movement log should be used to record all physical backup media movements.
- The location where physical backup media are stored should be secured from environmental hazards and be restricted to authorised personnel.
- All physical backup media should be stored securely in a locked fire-proof safe and access to the safe should be restricted to authorised personnel.

7.2. Disaster recovery policy

7.2.1. Objectives

The objective of this policy is to ensure that the critical business functions and underlying IT systems are recovered in acceptable times in the event of a disaster.

7.2.2. Guidelines

- CIEL should set up a Crisis Management Committee and Task Force to drive the creation, implementation and maintenance of a BCP. The planning should include members of the Executive Management as well as key representatives across all functional areas.
- CIEL should set up a risk assessment workshop to identify potential risks, and the probability of occurrence and potential impact to the organisation. Examples of key risks are loss of staff in key positions. As such, it is important to have a succession planning to respond to the absence of persons in key positions.
- CIEL should undertake a Business Impact Analysis to identify those processes that are critical to the continuity of business operations immediately after a disaster. Management should also determine how soon these key processes should be recovered following the disaster.
- CIEL should document the continuity strategy in terms of detailed procedures, key staff and resources required to recover critical processes. The strategy should include the disaster recovery of IT components (DRP) supporting critical processes;
- CIEL should identify and select the best recovery strategy, based on cost considerations of the different recovery strategy options and continuity strategies, taking into account existing capabilities.
- CIEL should develop awareness of the BCP through trainings and awareness sessions. The plan is communicated to relevant key staff of each functional department and a copy is kept at the offsite location.
- The IT Administrator and key business users with the approbation of Senior Management should perform a simulation on an annual basis to test the reliability of the plans (BCP and DRP) either for selected processes or for all critical processes with key stakeholders.
- The IT Administrator and the key business users should regularly review and update the plans in line with changes in the business and observations made during simulation exercises.

8. Governance of IT Security Management

8.1. Objectives

This policy aims at ensuring, establishing and monitoring security policies and standards.

8.2. IT Security Function and Governance policy

- The IT Administrator should continuously monitor the IT infrastructure to ensure compliance, reduce security threats and to implement appropriate solutions.

- CIEL should appoint an Information System Security Manager (ISSM) who will have the responsibility to establish, document and monitor the IT Security Function. The ISSM shall be in charge to report to the audit and reporting committee, and the following should be clearly defined:
    - Role
    - Responsibilities
    - Report to whom
    - Which control needs to be monitored.
- The ISSM will be responsible to implement an appropriate governance framework to manage all IT Governance, risk and compliance issues.
- The specific responsibilities of the ISSM are:
    - To implement, manage and develop the organization's IT security.
    - To synchronize information security inspections, tests and reviews.
    - Being responsible for data and network security processing.

9. Administration of IT Policies

9.1. Objectives

The objective of this policy is to ensure that the IT policies are formalised, regularly updated and communicated to all the relevant personnel.

9.2. Annual update guidelines

- There should be the implementation of annual review of IT strategy and specific policies which considers and make provision for changes which occurs in the organisational goals and IT environment.

9.3. Validation process

- All IT policies should be signed and approved by the Board
- Once the policies have been validated by the Board, they should be communicated to all employees, either by mail, verbally or by distributing copies of the policies.
- The policies should be retained on the Intranet where it is accessible to all authorised employees.

9.4. Declination by entities of the IT policy into local policies

- This IT policy details the minimum guidelines that should be followed, additional guidelines can be added in the event that specific requirements have to be met.

10. Data classification and protection of data

10.1. Objectives

The objective of this policy is to define the guidelines to classify data so that they can be easily accessed and protected . CIEL has a legitimate interest to process data including personal data and it is crucial that it complies with all applicable data protection laws including the Data Protection Act 2017 and the EU General Data Protection Regulations ("GDPR") (together referred to as "Data Protection Laws").

10.2. Data Classification

Proper classification of data is required and should be based upon the nature and sensitivity of the data. Classifying the data allows to apply specific controls and security measures to safeguard it.

Below is an indicative guideline to classify data:

- Highly restricted: these pertain to highly sensitive data which should not be disclosed externally.
- Confidential: pertain to less sensitive data which should not be disclosed externally.
- Private: This data should be circulated within CIEL only.
- Public: Information which can be shared outside the organisation

Data should be kept strictly confidential. Any unauthorised disclosure or accidental loss of data is likely to have a heavy impact on CIEL's reputation and if the disclosure is a violation of the law, may render CIEL liable to fines and/or possible civil claims for breach of data security. Disclosure of data :

- is permitted only to authorised persons on a "need-to-know" basis for purposes of performing a contract on the basis that the authorised persons are in turn bound to maintain the confidentiality of the data or
- with the prior to the owner's permission or
- as required by law.

10.3. Protection of data

This section applies to entities whereby CIEL has access to and processes third party information.

- CIEL should ensure that the confidentiality of all customer data regardless of classification is protected by means of an adequate access control and authorisation mechanism.
- All data removed from the CIEL's premises, for offsite backup reasons or the repair of hardware devices (PC's, laptops, servers), should be adequately secured and controlled before the release of the data from the premises.
- All sensitive data should be properly deleted from the media, including backups, with no residue remaining that could be recovered by unauthorised individuals.
- If confidential information is released orally in a meeting, seminar, lecture, video conferencing or other presentation, the speaker should clearly communicate the

sensitivity of the information. The speaker should also remind the participants to use discretion when disclosing it to others.

- Visual aids such as slides or overhead transparencies should include the appropriate classification markings. After the meeting, presentation materials whether IT-related or otherwise, e.g. flipchart sheets, pads, whiteboards, video, computer files, should be cleaned or removed from the meeting room.
- Only personnel, who were specifically invited to attend meetings where strictly confidential information will be discussed, should be present. Exceptions will be made only if advance management approval is obtained. Such meetings should be conducted in fully enclosed conference rooms.

10.4. Compliance to Data Protection Act (DPA 2017) & GDPR

Where CIEL collects, processes and manages personal data, which is information relating to an identified or identifiable individual (the data subject), it shall comply with the Data Protection Act 2017 (DPA), and such other applicable laws and regulations for the protection of personal data, including the EU Genaral Data Protection Regulations ("GDPR") ("together referred to as the "Data Protection Laws").

In order to comply to theData Protection Laws, CIEL should perform the following:

- Organise and assess existing data structure
- Adopt policies and implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in accordance with the Data Protection Laws. Such measures being:
  - Implementing appropriate data security and organisational measures;
  - Keeping a record of all processing operations;
  - Performing a data protection impact assessment where processing operations are likely to result in a high risk to the rights and freedoms of the data subjects;
  - Complying with the requirements for prior authorisation from or consultation with the Data Protection Commissioner (where applicable);
  - Designating an officer responsible for data protection compliance issues.

- perform an inventory of all personal data collected, processed and managed by it in order to determine the purpose for processing and retaining such personal data. All data should be classified and labelledwith due respect to their purpose and sensitivity.
- Conduct a data flow and identify data owners
- nominate a data protection officer who shall through the assistance of the IT Administrator monitor compliance of this IT Policy in roder to uphold data privacy within the organisation andprotect the integrity and confidentiality of data.
- Determine the purpose of the data being kept
- Adopt policies and implement procedures to ensure that personal data are:
  - collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes

  - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
  - processed in accordance with the rights of data subjects.
- Assessment of risks
- identify any probable threat of information disclosures and be prepared to counteract any security failure.
- Registration of data controllers and data processors
-
- CIEL should also implement procedures so as:
  - To make data protection a vital part of senior management's concern;
  - To allocate sufficient budget to data protection initiatives to depict commitment;
  - To include data protection into the core values of the organisation.
- CIEL should organise regular awareness trainings to employees on data protection and security and the consequences of unlawful data disclosure. Additionally, users should be made aware of the Data Protection Laws.
- CIEL should plan yearly compliance audits to ensure continuous compliance from employees to the policies and the Data Protection Laws. All instances of non-compliance should be reported to management and remediated.

11. Compliance

11.1. Objectives

This policy provide guidelines to deal with confidential and standard information of the employees.

11.2. Compliance to regulatory and group guidelines

- Compliance to all regulatory frameworks is vital to maintain the integrity of CIEL.
- There should be periodic compliance review of the policies.
- Users should adhere to information security policies and CIEL should ensure compliance to the policies.
- In addition to the guidelines provided in this policy, all personnel should comply with all guidelines pertaining to IT Security in the following:
  - The Code of Business Conduct
  - The Financial Intelligence and Anti-Money Laundering Act 2002 (FIAML ACT)
  - FATF 40 Recommendations and Eight Special Recommendations on Terrorist Financing

- National AML/ CFT Strategies
- DPA 2017
- The EU General Data Protection Regulations
- Any other guideline and/or policies enforced at CIEL

12. Physical Security

12.1. Objectives

The purpose of this policy is to ensure that sensitive areas, where information system and critical information processing facilities are located, are protected against unauthorised physical access, damage, theft, interferences and environmental threats which may result in unauthorised information access and/or disruption of business operations.

12.2. General guidelines

- Data room that house CIEL servers should be protected with physical security measures that prevent unauthorised access.
- Access to the server room should be restricted to authorised personnel only. Access to the server room should be granted after approval of the IT Administrator and access granted through an automated access control mechanism.
- Doors and windows connected to the server room should always be kept locked when unattended.
- All windows should be equipped with burglar proof mechanisms.
- Entry and exit points of the server room should be kept under camera surveillance.
- Non-business related visits to sensitive areas is strictly prohibited.
- All servers should be placed in racks in the server room.
- All maintenance of equipment found in the server room should be performed in the presence of the IT Administrator.
- The IT Administrator should maintain a log book of entries detailing the visits of the server room and the purpose of the visit.
- The server room should have a raised flooring to protect against flood.
- Food, drinks and smoking is strictly prohibited in the server room.
- Air conditioning units should be kept clean and maintenance checks should be done once a year.
- The server room should be equipped with appropriate devices controlling environmental parameters such as temperature monitors, humidity sensors, fire suppression systems (e.g. FM200 gas), smoke detectors, uninterrupted power supply, power generators. Fire extinguishers should be carbon dioxide or powder based.
- Inflammable materials such as discarded cardboard boxes should not be kept in the server room.

13. Security Monitoring

13.1. Objectives

This policy provides guidelines to ensure that CIEL's network is adequately protected and that usage is monitored.

13.2. Network usage monitoring

- Network access should be granted by the IT Administrator.
- There should be specific automated tools to monitor; internet traffic, electronic mail traffic and LAN traffic.

13.3. File access monitoring

- Users should not share their credentials (ID/password) with any other individual. Files with confidential and sensitive data need to be protected with a password to restrict access to any third party.
- Users need to be provided access to information which is only required for them to perform their official office related task. These information should be protected through login and password authentication.
- When a new staff joins CIEL, allocation of access right should be granted after following a process. The Human Resource and IT department should work together to grant the new joiner its user rights and access control, and their user profile should be entered in the system.

14. Cyclone

14.1. Objectives

This policy outlines the specific guidelines to be followed in the event of a cyclone.

14.2. Cyclone policy

- The IT Administrator should perform the following after obtaining the go-ahead by the Head of Finance:
  - Ensure that all data and applications for the day have been properly backup.
  - Ensure that the server room is protected from eventual water leakages.
  - Switch off all the servers in the server room and ensure that all workstations have been properly switched off.
- After the cyclone, the IT Administrator should perform the following:
  - Assess the state of the server room and identify any damages to equipment.
  - Request all staff to immediately inform him in the event that their workstations have been damaged.
  - Report to management about any incidents or damages to the equipment.

- The IT Administrator should ensure that all assets are covered by a valid insurance, so that CIEL can claim for compensation in event of any damages.

15. Mobile device

15.1. Objectives

This policy outlines the guidelines to safeguard both privately owned and company owned devices to prevent threats to IT and data security.

15.2. Bring your own device

- It is not encouraged to use personal devices (e.g. laptops) to connect to the organisation's network, data and systems.
- There are few exceptions where personal devices can be connected to CIEL network for a business need:
    - A request for the connection of a personal device to CIEL systems should be made to the IT Administrator and the business rationale which supports the request should be clear on the Bring Your Own Device Request Form.
    - Once the request has been approved, the IT Administrator should ensure that the personal devices comply with the applicable security requirements as per table below:

Function	Minimum requirement
Operating systems	The personal device must make use of an acknowledge operating system that meets the minimum standards defined in the related IT policies of CIEL.
Network authentication	The minimum network authentication should meet the requirements of CIEL's network security policy.
Password protection/ User authentication	The device should be in line with CIEL's password policy.
Antivirus solution	Appropriate and updated antivirus software should be installed on the device and it should comply with CIEL's antivirus policy.
Application	Only the applications authorised on CIEL's software whitelist should be installed.

- The connection of a personal device to CIEL Network without the written approval of the IT Administrator represents a breach of policy.
- The custodian of the personal mobile devices should agree to the terms and conditions set in this policy and he is responsible for ensuring the security of data held in the devices.

15.2.1. Risk, Liabilities and Disclaimer

- If a company email is used on a personal device, the same guidelines as on a company owned device should be followed.
- Any security incidents of unauthorised data access, data loss, or disclosure should be immediately reported to the IT Administrator. Refer to the IT Incident Management Policy.
- The users of the personal devices should bear full responsibilities of risks, for instance, the partial or complete loss of company or personal information due to a system crash, bugs, errors, malware or other failures.
- Appropriate disciplinary actions should be taken for any non-compliance with this policy.
- CIEL has the right to examine the personal devices and keep it in its custody in the course of investigation of any incidents.
- If users do not comply with this policy, CIEL reserves the right to disconnect the device to CIEL's network.

15.3. Mobile devices

- Mobile devices pertain to:
  - All company's or personal smartphone used by CIEL staff.
  - All IPads and other similar tablets used by CIEL employees.
  - All laptops used for the execution of daily duties
- A specific code of conduct should be applicable to any user of company mobile devices; which are as follows;
  - Being responsible to protect sensitive data stored on the device.
  - Being responsible to ensure physical safety of the device.
  - Being responsible of updating the software on the device.
  - Being responsible to report any theft or loss of company mobile devices immediately after being recognised to the concerned department so as to reduce further risk, avoid loss of data and information leakages.
  - Prohibition of tampering and removing any security controls which has been previously installed by the IT Administrator in the device.
  - Prohibition of copying sensitive information from the company mobile devices to any unapproved personal device.
  - Prohibition of conducting personal work from the company owned device.

15.4. Removable Media

- If an employee needs to use a removable media, a formal request should be made to the IT Administrator specifying the business reasons.

- Encrypted removable media should be used. In the event where it is not possible, the user should either password-protect the data or encrypt the information stored in the removable media.
- It is the responsibility of the employees to store the removable media in a secure environment in order to minimise the risk of loss or theft.
- Users of a removable media are responsible for the appropriate use of the device and for the security of data.
- For security purposes, it is not recommended that employees use the removable media devices for a long term storage.
- As soon as there is no need for data to be stored on the removable media, it is the responsibility of the employees to erase all the sensitive information from the removable media device.
- Prior to the disposal of the removable device, the users should make sure that any business critical information stored is erased. Refer to the IT Asset Disposal policy.

15.5. Smartphone

- An Acceptance of End User IT Policy form should be filled by all smart phone users who are required to connect to CIEL Network.
- Once the request has been approved, the IT Administrator should configure the smart phone to enforce all the approved security standards.
- Upon the approval from the Head of Department and from the IT Administrator, only approved smart phones should be connected and/or synchronise to CIEL device and network.
- In the event of loss or theft of the custodian's smart phone, the IT Administrator should be immediately contacted/ notified. The latter will be responsible to initiate the remote wipe out.
- Upon the termination of contract or employment with CIEL, the smart phone user should notify the IT Administrator who will wipe out all business data from the device.

15.5.1. Recommendations for International Travellers

- The smart phone users travelling overseas should bear all the expenses incurred for each megabyte of data the smart phone has used to receive or send data.
- Below are some recommendations that the smart phone users can follow in order to avoid huge data roaming charges:
  - Switch from automatic to manual synchronisation to the mail server to prevent the phone from being continually connected to the server.
  - Whenever possible, disable the data roaming services.
  - Purchase a local Sim Card in the country where they are that can be refunded by CIEL after prior arrangement with the relevant Head of Department.
- It is not recommenced to use public Wi-Fi connection due to security reasons.

15.6. Laptop Security

- The custodian is responsible for his laptop and related accessories, and should ensure that the device remains under his personal control.
- The laptop should be used for authorised business needs only.
- The custodian should take note of the laptop model and serial number. These will be useful to notify the IT Administrator in the event that the laptop is stolen or loss.
- On termination of services within the organisation, the custodian should return the laptop to the IT Administrator.
- The custodian is not allowed to install unauthorised software on the organisation's laptop.

15.6.1 Physical security

- It is advised that each custodian uses a cable lock to attach his laptop to his desk or similar furniture before leaving his desk.
- In order to avoid any accidental spills, it is recommended to keep food and drink away from the laptops.
- The laptops should be carried in a padded laptop bag so as to reduce any accidental damage.
- In the event that the custodian is travelling, he should always keep his laptop as a carry-on luggage.
- The laptop should always be locked when not in use.
- When leaving the office premises the laptop should either be taken by the custodian or kept in a safe and locked place for e.g. in a strong cupboard or locker.
- The custodian should never leave the laptop visible when unattended in a vehicle.

15.7. Printer and Scanner

Below are some guidelines to be followed by the employees:

- In order to minimise costs, multiple copies of the same document should not be printed.
- It is more cost effective to take advantage of the duplex printing features (double-sided printing)
- It is recommended to archive mails in folders rather than printing the e-mail messages.
- Printing in colour is less cost effective and it is preferable that employees use monochrome (black)
- It is not recommended that employees print large files as this can prevent others from using the printer. They should report any planned large files print jobs to the IT Administrator so that the most appropriate printer can be selected.

15.8. General confidentiality

- Information contained on CIEL's systems concerning the general business or operations should not be disclosed to any third party including competitors, members of the public, media, including social media or other CIEL employees not concerned by the information.

- Reports or any working documents should not be replicated without formal approval from the Board.
- Non-compliance to the above shall entail disciplinary actions or immediate dismissal.

Appendix A: Email Etiquette

- This section deals with the set of rules and appropriate social behaviour when using email as a means of communication, so as to avoid unwanted situations.
- Acceptable guidelines
  - All emails should be sent with a subject, and should be well structured and presented
  - All emails should include the sender's full name, job title and the company name
  - All emails should have white backgrounds
- In line with the antivirus policy, all employees should first scan their email attachments before opening them.
- It is highly recommended that employees should check the Email headers, especially if the employee has doubts about the Email or the authenticity of the sender. In such cases, if the employee considers the Email to be of suspicious nature, the employee should request the IT Administrator for assistance.

Appendix B: List of permitted software

Software whitelist	
Microsoft Office	Office documents and email
Acrobat reader	Reading and editing of PDF
7z	For compression of files
WinZip	For compression of files
WinRAR	For compression of files
Eazzy Filing	Filing system for documents
Sicorax	HR and Payroll
Navision	Old payroll system in read only now
Quickbooks	Accounting
Solis Accounting	Accounting
Solis TMR	Treasury Management
Sophos	Antivirus
Global Protect	VPN Client
Internet Explorer	Browser
Chrome	Browser
Firefox	Browser
Java Application	To run some other applications
All of the Microsoft approved software	

Appendix C: List of blocked websites

Categories of blocked websites

- Abortion
- Abused-drugs
- Adult-and-pornography
- Alcohol-and-tobacco
- Auctions
- Bot-nets
- Cheating
- Confirmed-spam-sources
- Cult-and-occult
- Games
- Gross
- Hacking
- Hate-and-racism
- Hunting-and-fishing
- Illegal
- Keyloggers-and-monitoring
- Malware-sites
- Marijuana
- Not-resolved
- Nudity
- Online-gambling
- Online-music
- Open-http-proxies
- Peer-to-peer
- Personal-sites-and-blogs
- Phishing-and-other-frauds
- Proxy-avoidance-and-anonymizers
- Questionable
- Religion
- Sex-education
- Shopping
- Social-networking
- Spam-urls
- Sports
- Spyware-and-adware
- Streaming Media
- Swimsuits-and-intimate-apparel
- Unconfirmed-spam-sources
- Violence
- Weapons

Appendix D: General recommendations from the Cyber Security Services report

The points below detail the recommendations from the Cyber Security Services report for CCS. Even though, they pertain to specific hosts, these should be taken as general guidelines and applied to all future hosts to ensure a highly secured infrastructure.

- The IT Administrator should enforce 2-factor authentication in the CIEL Office 365 portal.
- The IT Administrator should regularly assess the policies and access control for the firewalls on public facing infrastructure (routers from the different ISP (Mauritius Telecom & Emtel)).
- The IT Administrator should contact the vendor or consult product documentation to disable CBC (Cipher Block Chaining) mode cipher encryption, and enable CTR (or GCM cipher mode encryption.
- The IT Administrator should enforce 2-factor authentication and lockout on management interfaces which are publicly available via HTTPS, SSH and Telnet.
- The IT Administrator should perform a review of open firewall ports to ensure that only secure protocols are allowed to provide optimal protection against outside attacks.
- The IT Administrator should add a registry key named NtfsDisable8dot3NameCreation to the HKLM\SYSTEM\CurrentControlSet\Control\FileSystem and set the value of the key to 1 to mitigate all 8.3 name conventions on the server.
- The IT Administrator should disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.
- The IT Administrator should ensure that SSLv2 protocol is disabled in all their SSL/TLS servers to prevent against DROWN attacks.
- The IT Administrator should ensure that RC4 cipher suites is not used in TLS connections.
- The IT Administrator should disable SSLv3 and replace it with TLSv1.0 as soon as compatibility with legacy clients is no longer required in order to prevent POODLE attacks.
- The IT Administrator should determine if HTML form requires CSRF (cross-site request forgery) protection and implement CSRF countermeasures if necessary.
- The IT Administrator should ensure that all password fields on webpages should be submitted through POST instead of GET method.
- The IT Administrator should ensure that all SSL certificates have a key length of at least 2048-bit.
- The IT Administrator should ensure that CIEL has the latest version of the JavaScript library.
- The IT Administrator should ensure that versions 1.33 and/or 1.5 of the SSH protocol are not used since they are not completely cryptographically safe.
- The IT Administrator should disable the Telnet service and use SSH instead.
- The IT Administrator should ensure that all web servers are up-to-date to prevent cross-site scripting attacks.
- The IT Administrator should ensure that all SSL certificates that have been signed using a weak hash algorithm are re-issued.

- The IT Administrator should ensure that all certificates are signed by a known public certificate authority.
- The IT Administrator should ensure that all HTTP servers have the Apache version 2.0.65 / 2.2.22 or later so that they are not prone to the information disclosure vulnerability.
- The IT Administrator should ensure that theMD5 and 96-bit MAC algorithms are disabled since they are weak.
- The IT Administrator should ensure that web servers include an X-Frame-Options header to prevent from Clickjacking attacks.