GEECEE FINCAP LIMITED

INFORMATION TECHNOLOGY POLICY & PROCEDURAL MANUAL

(Effective Date: 30th March, 2024)

Reviewed & Updated by the Board of Directors

Table of Contents

(Updated Version – 30th March, 2024)

-Adopted by the Board w.e.f 23rd May, 2018
-Reviewed by the Board on 08th August, 2022
-Amended by the Board w.e.f 03rd February, 2023
-Reviewed and amended by the Board w.e.f. 30th March, 2024

Introduction

GeeCee Fincap Limited ('the Company' or 'GCFL') Information Technology ('IT') Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the organisation which must be followed by all staff. GCFL will use to administer these policies, with the correct procedures to follow.

GCFL will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All policies must be periodically reviewed for appropriateness by the IT Committee.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

A. Technology Hardware Purchasing Policy

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the organisation to ensure that all hardware technology for the organisation is appropriate, value for money and where applicable integrates with other technology for the organisation. The objective of this policy is to ensure that there is minimum diversity of hardware within the organisation.

Procedures

1. Purchase of Hardware

a. Purchasing desktop computer systems

The desktop computer systems purchased runs with the latest operating system and integrate with organization server.

The desktop computer systems must be purchased as standard desktop system bundle and it must mention all the details like serial no, Ram, Hard Disk, CPU, LCD Size etc.

The desktop computer system bundle must include (below are the standard configuration):

i. Desktop or Tiny Desktop
ii. Desktop screen of {20 or 21'}
iii. Keyboard and mouse
iv. Windows 10 and above and Ms office 2010 and above
v. If Required such as speakers, microphone, webcam, printers etc.
vi. The minimum capacity of the desktop must be:
    Cpu Speed I(3) and above 3.4 and above GHz –gigahertz
    240 GB or above SSD Hardrive
    4 GB or 8 GB or above
    4 Usb port USB port and 1 hdmi port
    If required such as DVD drive, microphone port, etc.

All purchases of desktops must be supported with warranty and be compatible with the organization's server system.

b. Purchasing portable computer systems

The purchase of portable computer systems includes Ipad, notebooks, laptops, tablets etc. Portable computer systems purchased runs with the latest operating system and integrate with organization server.

The portable computer systems purchased must be from reputed companies like Dell, Lenovo,HP, etc.

The minimum capacity of the portable computer system must be:
1. Cpu Speed 3.4 and above GHz –gigahertz
2. 500 GB SSD or above
3. 8GB or 16 GB

4. 2 USB ports and 1 HDMI port
5. If required such as DVD drive, microphone port, etc.

The portable computer system should have all required software as per the requirement of user which includes MS Office 2013 and above, Internet Explorer 11 and above, any specific software with prior permission from management.

All purchases of desktops must be supported with warranty and be compatible with the organization's server system.

2. Purchasing server systems

Server systems can only be purchased as per the requirement of Management or for new business set up, if any.

Server systems purchased must be compatible with all other computer hardware in the organization.

All purchases of desktops must be supported with warranty and be compatible with the organization's server system.

3. Purchasing computer peripherals

Computer system peripherals include printers, scanners, external hard drives, Pen drive etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software in the organization.

All purchases of desktops must be supported with warranty and be compatible with the organization's server system.

Note: Any above purchase must be approved by appropriate authority by signing on fixed assets requisition form. This form will be filled by IT person with approved budget & reason for purchase.

B. <u>1. Policy for Getting Software</u>

Purpose of the Policy

This policy provides guidelines for the purchase of software for the organization to ensure that all software used by the organization is appropriate, value for money and where applicable integrates with other technology for the organization. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

Procedures

1. **Request for Software**

   Any required software must be approved by proper authority by signing on fixed assists requisition form. This form will be filled by IT person with proper budget & reason for purchase.

2. **Purchase of software**

   The purchase of all software must adhere to this policy.

   All purchased software must be purchased from appropriate or well-known vendor.

   All purchases of Software must be supported with proper AMC and must be supported with warranty and be compatible with the organisation's server system.

3. **Obtaining open source or freeware software**

   Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

   In the event that open source or freeware software is required, prior approval must be obtained from IT personnel for downloading or for using such software.

   All open source or freeware must be compatible with the organisation's hardware and software systems.

4. **Update**

   All the purchased software must be properly updated to latest version available.

B. 2. Policy for Use of Software

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the organization to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

1. **Software Licensing**

   All computer software copyrights, and terms of all software licenses will be followed by all employees of the organization.

   Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of IT Person to ensure these terms are followed.

   IT Person is responsible for completing an IT audit of all Computer system once a year to ensure that software copyrights and license agreements are adhered to.

2. Software Installation

All software must be appropriately registered with the supplier where this is a requirement.

Only software obtained in accordance with the getting software policy is to be installed on the organisation's computers.

All software installation is to be carried out by IT Person.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

3. Software Usage

Only software purchased in accordance with the getting software policy is to be used within the organization.

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of IT Person.

Employees are prohibited from bringing software from outside the organisation and loading it onto the organisation's computer hardware.

Unless express approval from Management is obtained, software cannot be taken outside the organisation and loaded on an employees' personal computer.

Where an employee is required to use software outside the organisation an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's personal computer, authorization from Management is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the organization and must be recorded on the software register maintained by IT Person.

Unauthorised software is prohibited from being used in the organisation. This includes the use of software owned by an employee and used within the organisation.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to IT Person for further consultation, reprimand action etc. The illegal duplication of software or other copyrighted works is not condoned within this organisation and IT Person is authorised to undertake disciplinary action where such event occurs.

4. **Breach of Policy**

   Where there is a breach of this policy by an employee, that employee will be referred to IT Person for reprimand action.

   Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify IT Person immediately. In the event that the breach is not reported, and it is determined that an employee failed to report the breach, then that employee will be referred to IT Person for any consequences.

C. Bring Your Own Device Policy

At GCFL, we acknowledge the importance of technologies in improving organisation communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own devices to GCFL network and equipment. This can be permitted after prior approval from management. Following are the list of owned assets which may be used by the employee for office work:

1. Laptop
2. Smart phones / iPhone
3. Tablets
4. Removable media
5. Any other assets which may be permitted by management after consulting with IT Persons.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets for organisation purposes. All staff who use or access GCFL technology equipment and/or services are bound by the conditions of this Policy.

Procedures

1. **Current mobile devices approved for organisation use**

   The following personally owned mobile devices are approved to be used for organisation purposes:

   As per the specification of work & the requirement of team, management will permit to use various devices like notebooks, smart phones, tablets, iPhone, removable media etc.

2. **Registration of personal mobile devices for organisation use**

   Employees when using personal devices for organisation use will register the device with IT Person.

   IT person will record the device and all applications used by the device.

   Personal mobile devices can only be used for the following organisation purposes:

   1. Email,
   2. Wi-Fi,

3. Telephone call

Each employee who utilizes personal mobile devices agrees:

Not to download or transfer organisation or personal sensitive information to the device. Sensitive information includes property & other employee details etc.

Not to use the registered mobile device as the sole repository for GCFL information. All organisation information stored on mobile devices should be backed up. To make every reasonable effort to ensure that GCFL information is not compromised using mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected.

To maintain the device, it should be maintained with current operating software, current security software etc.

Not to share the device with other individuals to protect the organisation data access through the device.

To abide by GCFL internet policy for appropriate use and access of internet sites etc.

To notify GCFL IT Team immediately in the event of loss or theft of the registered device.

Not to connect USB memory sticks from an untrusted or unknown source to GCFL equipment.

All employees who have a registered personal mobile device for organisation use acknowledge that the organisation:

1. Owns all intellectual property created on the device
2. Can access all data held on the device, including personal data
3. Will regularly back-up data held on the device
4. Will block all data held on the device in the event of loss or theft of the device
5. Has first right to buy the device where the employee wants to sell the device
6. Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data.
7. Has the right to deregister the device for organisation use at any time.

3. Keeping mobile devices secure

The following must be observed when handling mobile computing devices such as notebooks and Ipad

Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away.

Cable locking devices should also be considered for use with laptop computers in public places, e.g., in a seminar or conference, even when the laptop is attended.

Mobile devices should be carried as hand luggage when travelling by aircraft.

4. **Staff Device Policies**

   If any employee of the company wishes to give their desktop / laptop or any other device to IT personnel for repairs, the same can be done with prior permission from the Management.

5. **Outsider Device Policies**

   Similarly, if any other person besides employee of the company (i.e. visitor / relative of the employee) wish to give their equipment i.e. computer, laptop for maintenance / repair or even wish to access internet, then the same will be permitted with prior permission from the Management.

6. **Access to Auditors**

   Any access of software, files, folders, if any, given to auditors must be approved by management.

7. **Breach of this policy**

   Any breach of this policy will be referred to IT Person who will review the breach and determine adequate consequences, which can include serious consequences here such as confiscation of the device and / or termination of employment.

8. **Indemnity**

   GCFL bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnifies GCFL against any and all damages, costs and expenses suffered by GCFL arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by GCFL.

D. <u>Information Technology Administration Policy</u>

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the organisation.

Procedures

All software installed and the license information must be recorded properly with each & every details. It is the responsibility of IT Person to ensure that this register (in form of folders) is maintained. The register must record the following information:

1. Licenses details
2. Software key

3. User name & passwords
4. Renewal dates

IT Person is responsible for the maintenance and management of all service agreements for the organisation technology. Any service requirements must first be approved by Management.

IT person is responsible for maintaining adequate technology spare parts and other requirements like Ram, Hard Disk, etc.

E. Website Policy

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the organisation website.

Procedures

1. Website Content

All content on the organisation website is to be accurate, appropriate and current. This will be the responsibility of Company Secretary

All content on the website must follow relevant organisation requirements where applicable, such as an organisation or content plan etc.

The content of the website is to be reviewed time to time basis.

The following persons are authorised to make changes to the organisation website:

Company Secretary and any of the Directors of the company

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the organisation.

2. Website security

The Company web sites must maintain a secure configuration that enables the site to resist common attacks. The IT Manager will be responsible for establishing and maintaining this configuration based on common standards.

F. Electronic Transactions Policy

Purpose of the Policy

This policy provides guidelines for all electronic transactions undertaken on behalf of the organisation.

The objective of this policy is to ensure that use of electronic funds transfers and receipts are started, carried out, and approved in a secure manner.

Procedures

1. **Electronic Funds Transfer (EFT)**

   It is the policy of GCFL that all payments and receipts should be made by EFT where appropriate.

   All EFT payments and receipts must adhere as per the proper system as decided by the Management.

   All EFT arrangements, including receipts and payments must be submitted by inputters to the authorized persons for authorizing the transactions.

   EFT must have the appropriate authorization for payment or receipts. Any payment or receipts must be properly authorized by one from two senior persons from Management. The password for authorization must be kept secret between these persons.

   EFT payments once authorized, will be entered into the financial related software like Tally & it will be signed by inputter & authorized persons. EFT payments can only be released for payment once pending payments have been authorized by authorized persons.

   For good control over EFT payments, ensure that the persons authorizing the payments and making the payment are not the same person.

   All EFT payments or receipts must be reconciled to online bank statement at the end of every day by the inputter, in case any discrepancy, then inputter has to inform to the authorized person immediately.

   Where EFT receipt cannot be allocated to customer account, it is responsibility of accountant to investigate. In the event that the customer account cannot be identified within specified period as decided by Management, the receipted funds must be allocated to suspense account & must authorize this transaction.

2. **Electronic Purchases**

   All electronic purchases by any authorized employee must be approved by the Management.

   Where an electronic purchase is being considered, the person authorizing this transaction must ensure that the internet sales site is secure and safe and be able to demonstrate that this has been reviewed.

3. **Electronic Transaction Security**

   Group has policy of Maker-Checker in case of all the electronic transaction.

G. IT Service Agreements

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the organisation.

Procedures

The following IT service agreements can be entered into on behalf of the organisation:

1. Computer & Printer AMC
2. FM Charges (Engineering Charges)

All IT service agreements must be reviewed by IT person before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Management.

All IT service agreements, obligations and renewals must be recorded. Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorized by IT person.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, IT Person should review before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Management.

IT person must review every area of IT after a specific interval say, every year & give proper recommendation for any updation.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to Management who will be responsible for the settlement of such dispute.

H. Emergency Management of Information Technology

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the organisation.

Procedures

1. IT Hardware Failure

Where there is failure of any of the organisation's hardware, this must be referred to IT Person immediately.

It is the responsibility of IT Person to undertake tests on planned emergency procedures to ensure that all planned emergency procedures are appropriate and minimise disruption to organisation operations.

2. Virus or other security breach

In the event that the organisation's information technology is compromised by software virus or any breaches of data, hard disk crash such information are to be reported to IT Person immediately.

IT Person is responsible for ensuring that any security breach is dealt with within relevant timeframe to minimise disruption to organisation operations.

I. Biometric Attendance Monitoring Policy

Purpose

This Policy helps to maintain the staff in & out records.

Procedure

a) Attendance Rules

1. The Biometric Attendance Monitoring System is being maintained for the record of attendance. Employees of the group will be required to mark In and Out in the Biometric Attendance Monitoring System machine. First and last enrolment to the system will be considered for attendance purpose.

2. HR will send attendance record to all employees **at the end of the month at employee's** email id. Every employee should check his /her details & approve the same. If there is any issue, he / she will immediately inform to HR **verbally and also through mail**.

b) Office Timings

1. Regular Office timings are 10.00 am to 06:00 pm (According to shift timings allotted) and lunch break **between 1pm – 2pm**.

2. Grace Period of 15 minutes is allowed for arrival only.

3. If the employee attends office beyond 15 minutes of the commencement of office hours and / or leaves before closure of the office hours, the system will record the attendance as LATE.

4. Any Late In or Early Out shall be deducted from leaves or salary as per decided.

5. If an employee arrives late / leaves early for more than 3 instances then he/she will be marked as half day leave on the fourth instance and next on seventh instance and then from 8th instance half day for every instance he/she is late/early (for eg. if an employee is late for 3 times in a month than he will be marked leave for ½ day for 4th late mark ,then again ½ day for 7th late mark and then if late more than 7days then half day for every late/early).

6. If any employee is out for personal work he/she will require approval from supervisor & also punch Out/In in biometric system **and also mention the same in Staff register maintained at Reception**.

7. If any employee wants to work on holidays then such employee must take prior approval from the management.

J. Information Technology Security Policy

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the organisation to ensure integrity, confidentiality and availability of data and assets.

Procedures

1. Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access. No person other than IT can allow entering in server room. The Server Room shall be only accessible through Biometric Devices.

It will be the responsibility of IT Person to ensure that this requirement is always followed. Also, it is the responsibility of all employee to take permission from IT person before enter into server room. Any employee becoming aware of a breach to this security requirement is obliged to notify IT Person immediately.

All security and safety of all portable technology will be the responsibility of the employee who has been issued with the device. Each employee is required to use security system like lock, password etc and to ensure the asset is always kept safely to protect the security of the asset issued to them.

In the event of loss or damage, IT Person will assess the security measures undertaken to determine if the employee will be required to reimburse the organisation for the loss or damage.

All electronic devices when kept at the office desk are to be properly secured by user of such device.

2. Information Security

a. Purpose:

This policy provides guidelines for the protection and use of information technology assets and resources within the organisation to ensure integrity, confidentiality and availability of data and assets.

b. Scope:

This policy applies to all Employees & Interns/Trainees of the Company, Group Companies and third party service providers.

Scope of this Information security Policy is the Information stored, communicated and processed within the Company and Company's data across outsourced locations.

c. Ownership & Responsibility:

To avoid conflict of interest formulation of policy and implementation / compliance to the policy to remain segregated. Therefore the IT Personnel will be responsible for implementation of IT Security Department.

The Chief Information Security Officer (CISO) will be responsible for articulating the IS Policy that the Company uses to protect the information assets apart from co-ordinating the security related Issues within the organization as well as relevant external agencies.

The CISO will be a senior level executive (preferably in the rank of a General Manager or an equivalent position) and shall not have any direct reporting relationship with the Head of IT function.

d. Policy Compliance Check:

All sensitive, valuable, or critical organisation data is to be backed-up every day by third party software (Auto Schedule). It will be the responsibility of IT Person to ensure that data back-ups are conducted weekly and the backed up data is kept at place outside the office. All technology that has internet access must have anti-virus software installed. It is the responsibility of IT Persons to install all anti-virus software and ensure that this software remains up to date on all technology used by the organisation. Access of software, hardware, Pen drive / CD Drive etc. is available only after proper prior approval from Management Otherwise pen drive /CD Drive is blocked for all PC's except PC's handle by Management / IT. All information used within the organisation is to adhere to the privacy laws and the organization's confidentiality requirements.

e. Penal Measures for Non-Compliances:

Any employee breaching this will be liable for Penal action.

f. Periodic Review:

The policy shall be reviewed periodically or at the time of any major change in existing IT environment affecting policy and procedures and placed before the Board for approval. This policy will remain in force until next review / revision.

3. Technology Access

Every employee will be issued with a user id to access the organisation data and will be required to set a password to access data. The password will be under control of IT Person.

Each password is to be set with specific character & alphabets and is not to be shared with any employee within the organisation.

IT Person is responsible for issuing the identification code and initial password for all employees.

Where an employee forgets the password after various attempts, then IT Person is authorised to reissue a new initial password from his login id that will be required to be changed when the employee logs in using the new initial password.

The following table provides the authorization of access:

Technology	Persons authorised for access
Hardware	IT Person
Software	IT Person
Biometrics	IT Person / HR
CCTV	IT person/ HR/ Appropriate Management

Employees are only authorised to use organization computers for official work only. It is the responsibility of IT Person to keep all procedures for this policy up to date.

4. Data Transfer/Printing:

1. Electronic Mass Data Transfers:

Downloading and uploading, Confidential, and Internal Information between systems must be strictly controlled. All mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Applicable Business Associate Agreements must be in place.

2. Other Electronic Data Transfers and Printing:

Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. Confidential information must not be downloaded, copied, or printed indiscriminately or left unattended and open to compromise. All other data transfer website (like we transfer etc) is blocked for all staff. It can be available after prior approval of Management.

5. Remote Access

Access into GCFL network from outside will be granted using GCFL approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the GCFL network.

6. Risk Management

A thorough analysis of all GCFL information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the Group level.

Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

7. Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

A. Confidential Information

1. Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

   Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for organization, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

B. Internal Information

1. Internal Information is intended for unrestricted use within organization, and in some cases within affiliated organizations such as organization business partners. This type of information is already widely distributed within organization, or it could be so distributed within the organization without advance permission from the information owner.

   Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

2. Any information not explicitly classified as PHI, Confidential or Public will, by default, be classified as Internal Information.

3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

C. Public Information

1. Public Information has been specifically approved for public release by a designated authority within each entity of organization. Material posted

to companies of web site entity internet web pages are the example of Public Information.

2. This information may be disclosed outside of organization.

K. Back up Policy

Purpose of the Policy

This Policy provides the guidelines regarding the important back up of the organization.

Procedure

1. **Backup Media**

   Depending on the nature of the files being backed up, any of the following media may be used: external hard drive, a third party provider of an online backup service, if any, or the company's central backup system, if any for this purpose.

2. **Accountability**

   The requirements for backup will vary depending on many factors. It is the responsibility of IT Department to write and implement its own backup strategy. It should indicate:

   - The frequency of backups
   - The type of backup created (full or incremental)
   - The backup software / medium used
   - The location of off-site backup copies
   - The nature of logs kept
   - An individual or group assigned to monitor success and failure of backups

3. **Back-up of Data**

   a. **Backup Schedule:**

      i. Backup of **critical data** will be taken every Tuesday and Friday morning during business hours. This back up can be taken by using external hard drive. This back up data will be stored in other office premises i.e. outside the office premises. This is manual backup taken by IT person. This data will be kept date wise & will retain for six months. The period can be changed by Management based on the requirement.

      ii. Apart from this some of following **important data** are taken every day for back up on third party software as per schedule.
      The above back up starts automatically as per fixed schedule & the email alerts are received by IT person regarding successful completion or if there are any errors. If there is any error then appropriate action will be taken by IT person. This Back up data will override the earlier data taken by IT person.

      iii. Back up of **User's data** will be taken once in 15 – 20 working days, such back up data will overwrite the old back up. This back up can be taken by

using external hard drive. The User data backup includes the following items:

1. Desktop
2. Documents
3. Outlook
4. Any Drive

b. Data back up access must be restricted to IT person only.

c. All such back up data should be kept for 6 months as per the management decision which can be extended as per the requirement.

d. **Back up restoration policy**

The rights of restoration of back up data are with ONLY IT person. In case of emergency, details or procedure of such restoration can be explained to any other staff of origination (other than IT person).

e. **Additional Backup on Cloud-Based Storage Platform**
It has been decided during the financial year 2022-2023 to undertake Backup and Storage of Data on Cloud-Based Storage Platforms. The Data Backup and Storage Schedule on Cloud Platforms shall be on an Incremental Basis at One-Half Hourly Basis and will start its operation from 09:30 AM till 07:00 PM only on Week Days. On Saturday there shall be a Full Back up. The total Period during which the Data is stored on Cloud Platform is 2 months, post facto the data is fully deleted and a new Set of Backup and Storage Activities are operationalized. This Cloud Based Services ensures vulnerability assessment of data in addition to but not limited to Backup and Storage of Data. Further, this shall be in addition to the Conventional Method of Backup and Storage of Data on an External Hard Disk Drive.

4. Disaster Recovery Plan / Policy:

1. Firewall

If the Sonicwall firewall is down, then we have configured WIFI router as a switch so that it will work in network. If possible we can change IP also in server and client desktop. It takes maximum 15-30 minutes for network UP. IT team shall be responsible regarding the same.

2. Internet Wan Failover

We have three internets Lease line

- Bharti Broadband : 1 Tb
- Jio broadband : 1 Tb
- Hathway Lease line : 30 Mbps
  If any internet will be down, then firewall does auto switch in 2nd Internet Lease line

3. **Switch**

   If switch failover happens then we have a Standby switch in IT Team, if any switch has major issues in premises we will replace the switch immediately. This activity may take approximately 15 Minutes. IT team shall be responsible regarding the same.

4. **Tally server**

   - We restore data of the last day as backup
   - One day backup is to be restored
   - Tally and other document will be started in 30 Minutes
   - If server is down we will try to find out issues, if any hardware issue then we will discuss with Management at first and accordingly decision shall be taken.

5. **Desktop**

   - User desktop is down for any hardware issue and/or Windows issue then we shall provide a standby desktop
   - It may take approximately 30 Minutes

6. **WIFI**

   - If any WIFI router is down first of all we will find network issue or cable issue after that we will reset the wifi router. Even after that if it is not working then we will replace router (IT team do have standby router)

7. **UPS**
   - If UPS is down for any issue like battery or ups power issue
   - At First we will switch from UPS to power then we will raise issue to UPS technical team

8. **Telephone Line**

   - We have two PRI line in our organisation
   - Airtel PRI Line: Primary
   - Tata PRI Line: Secondary
   - MTNL Line telephone have been installed at Promoters Cabin, Director Room

   If Airtel PRI down then TATA PRI line will work and all TATA PRI call arrives at Reception Area. If EPPS is down then we raise issue with the Telephone Department

9. **CCTV**
   - We have 8 Camera and 2 DVR in the premises
   - If any camera and DVR is down then we will raise issue with Technical Team
   - IT Team needs to inform the Management about the issues
   - IT Team shall take keep 3 Months CCTV Backup as decided by the Management.

L. Email Policy

Purpose

This Policy provides the guidelines regarding Email domain of the origination.

Procedure

The GCFL has domain name called "gcvl.in" with netcore having 20GB space. The group has no in-house server & therefore all the mail are store on clouds. The incoming & outgoing size of mail box is 30MB for all devices.

For data security, there is agreement of security of data between Clouds & Group. Every year on 19th June the clouds email gets expired & gets renewed.

On reaching 70% of clouds email box of each user, alert will be sent to IT person Email id so that IT person can clear the mail id of user.

Email service provider: netcore

- Domain name: gcvl.in
- Domain name: geeceefincap.com
- gcvl.in: 150 users / active : 143 user
- geeceefincap: 10 user / Active : 7 User

gcvl.in email server is cloud based server all Email id is pop account
geeceefincap email server is cloud based all email id is pop account

We have taken extra services in gcvl.in domain only
ATP Protection: Advance treats Protection

ATP protection is spam email blocked as per netcore score policy
If any email blocked by ATP Protection then user get alert in half and hours and these email blocked by spam
User will first send email to IT team then only IT team will release these email
For release of this email from spam IT Personnel will be asked user name and password
Only IT team shall know the user name and password for release email
If email id is genuine then we add it in whitelist, next time email will not be blocked by spam server
Admin panel shall be logged in daily and monitored by IT team
Admin panel password shall be changed in 2 month
Company shall keep alerts in outlook for password reset

Cloudmail server – gcvl.in domain
Cloudmail server is using where we can create email id – reset user password-group email id – email size alert- outgoing email blocked who left organisation – All mail report
User and IT team get alerts after inbox reached 80% for increased size or delete email from cloud
Admin panel password we changed in 1 month – admin panel (as per now)
We keep alerts in outlook for password reset

DMARC : Secure your domain from email and Phishing attacks
We make rules for email who left the organisation in email server

We add email id in group then particular email id cannot send any email to outside and email send in gcvl.in domain

HR inform to IT Team who leaving the organization and also we made a 'Exit Form' with HR team.

M. Antivirus Policy

Purpose

This Policy provides the guidelines regarding Antivirus policy of the Organsation.

Procedure

KASPERSKY ANTI VIRUS – Rules & Regulations

We have created three groups for Kaspersky:

1) USB permitted version.
2) USB blocked version.

Policy details for above groups as below:

Application *Start-up Control to Enable* in above groups
Application *Privilege Control to Enable* in above groups
Vulnerability Control to Disable in above groups
Web Browser to Enable in above groups

- **Antivirus Protection rules in above groups** - General Protection setting - Monitored Ports - Monitor only selected ports.
- **File Antivirus rules in above groups** - File Antivirus Enable in above groups (untick only in All Network Drives).
- **Mail Antivirus rules in above groups** - Mail Antivirus Enable in above groups (scan only incoming email messages).
- **Web Antivirus rules in above groups** - Not to add any website in trusted applications.
- **IM Antivirus rules in above groups**.
- **System Watcher rules in above groups** –
- **Firewall rules in above groups** - Firewall to be enabled.
- **Network Attack Blocker rules in above groups** –in case of virus attack in network / computer, then Kaspersky will block the same within 15 minutes.
- **Bad USB Attack Prevention rules in above groups** –if faulty keyboard is used, then Kaspersky will not allow to access.
- **Advance setting rules in above groups**- Password Protection enabled in above groups - pen drive cannot be accessed until and unless user name &password is put and the same will start auto scan.
- **Reports and Storage rules in above groups** -email notification enabled in above groups will feature in **'shamim@gcvl.in'.**
- **Update Task rules in above groups** - Kaspersky Admit Kit Download update sand repository every hour. User update schedule – every two hours.
- **Scanning Task Schedule in particular department and group**–
  - Server scanning will be done every Thursday during morning hours.

- Office PC scanning will be done every Saturday. In case Saturday is off, then manual scanning will be done as and when possible.

N. Password Policy

Purpose

This Policy provides the guidelines regarding Password policy of the Organsation.

Procedure

Password Protection

All users and servers have individual desktop passwords (given by user), which have been shared with the IT personnel.

Users cannot change their passwords and the same will not expire.

Screen times out in 15 minutes in selective PCs.

1. Never write / store passwords.
2. Never send a password through email.
3. Never tell anyone your password.
4. Never reveal your password over the telephone.
5. Never put a 'hint' for your passwords.
6. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
7. If anyone asks for your password, refer them to the IT personnel.
8. Additional User Accounts have been created for each user which will be as a backup in case the user forgets the password or anything happens to the desktop / computer. These additional User Accounts are also password protected and only the IT personnel can access the same. The Additional user account can be accessed by IT person from each users machine.

Where an employee forgets the password after various attempts, then IT Person is authorised to reissue a new initial, password from his login id that will be required to be changed when the employee logs in using the new initial password.

All password of excel, word & statutory site & any other will be store on particular place & never share with anyone. Incase if user forgot any password of Microsoft word or excel then we have to use third party software to recover the data.

O. Expiry Policy

This Policy provides the guidelines regarding Expiry policy of the Organsation resources.

Policy Statements

The following table maps basic user privileges and expiration of privileges given.

Classification	Privileges	Expiry
Regular Full-Time Employee	• Company based desktop PC & laptop with approved software suite.	Date of termination of employment.

	• IP account for electronic mail and Web browsing (including intranet). • Access to shared work server and main shared applications server.	
Part-Time Employee, if any	• Company based desktop PC with approved software suite. • IP account for electronic mail and Web browsing (including intranet). • Access to shared work server and main shared applications server.	Date of termination of employment.
Internship	• Company based desktop PC with approved software suite. • IP account for electronic mail and Web browsing (including intranet).	Official end date of internship.

P. Employee Termination Policy

This checklist explains the employee departure checkout process. Follow these steps for any employee departure, whether voluntary or involuntary. This checklist assumes that appropriate written notification of pending departure has either been supplied by the employee in the event of resignation, or will be supplied to the employee in the event of termination.

1. Notify Human Resources.

2. Human resources should notify the appropriate personnel in IT in advance that an employee will be departing so that they can take appropriate security measures. Notify IT that all of the employee's accounts (network, e-mail, and voice) will need to be deactivated during the closing hours of the employee at a specific date and time. After the employee termination, for certain time, his/her email will be diverted to management people and after some time then his / her id will be deactivated.

3. IT and Human resources pull the documentation showing what company assets are assigned to the employee and must be returned.

4. Conduct an exit interview. At this interview, the following must be addressed:

    a. Review final compensation procedures and timeframe, including payout of any vacation pay accrued.
    b. Review termination date of any and all benefits, and any provisions for temporary extension of benefits.
    c. Review any confidentiality and non-disclosure requirements.
    d. Remind employee that all files and documents are company property and cannot be destroyed, removed, modified, or copied without approval from the direct supervisor.
    e. Ensure return of all company property to the employee's supervisor, or make arrangements for its immediate return. Company property includes all keys, access cards, identification cards, credit cards, tools, books, reference materials, software, and equipment (such as laptop computers, personal digital assistants, pagers, and

cell phones). This also includes all information, records, correspondence and documents about the Company and its clients.

f. Have the employee disclose all usernames and passwords to all accounts and/or applications to the employee's supervisor for records management and redistribution purposes.
g. Review the status of any and all projects or work in progress.
h. Have the employee disclose the location of key work-related documents and records.

5. All personal items, such as plants and family photos, must be removed from the employee's work area by the employee as close as possible to the time of employee departure. Under stressful circumstances, arrangements can be made for employees to clear out their personal items during off hours, or for the employee's personal belongings to sent to him/her by HR.

6. Arrange for the departing employee's e-mail and phone calls to be temporarily forwarded to the employee's supervisor, or other person designated by the employee's supervisor.

Employee Checkout Check List

Employee name:_____ Date:_____ Checkout Manager

Signature:_____

Handover Report	
Name	
Designation	
Department	
DOJ	
DOL	
Responsibilities Handover to Department	
Work Related Handover	
Files/Folders	
Handover Given to	
Handover taken by (remarks if any)	
Pending Work	
Name & Signature Department Head	
Comments by Department Head	
IT Related	
Software ID & Password	
PC Password (if any)	
Deactivation of Email ID	
All official emails access on any type of owned device must be deleted (Yes /No)	
Any Other Company Related ID or Password	
Name & Signature of IT Person	
HR/Admin	
Stationery	
ID Card	
Assets (Laptop/Pen drive, etc.)	

Name & Signature of HR/Admin	
Signature of Director	

Exit Interview	
How was your experience in Company	
Reasons for Leaving the company	
How is the Management Style working	
Your Suggestions for Improvement	
What you didn't like	
Feedback for Immediate Superior Immediate Superior Name :	
Are you Willing to rejoin in future	
Any more comments	
Exit Interview taken by (Name & Designation)	
Employee Signature	

Q. Business Continuity Policy & Disaster Recovery Policy

Purpose

This policy defines the requirements for developing, testing, and maintaining the business continuity plan.

Business Impact Analysis

The Information Security Department must perform a business impact analysis (BIA) each year after the annual organization-wide risk assessment. At the very least, this BIA must result in the specification of: the maximum period that GCFL can go without critical information processing services, the time period in which management must decide whether to move to an alternative processing site, and the minimum acceptable production information systems recovery configuration.

As part of the systems development cycle, all computer information systems must be evaluated by information security specialists to determine the minimum set of controls, the cost/benefit of such controls and the budget required to mitigate and maintain risk at a level acceptable to the business process(es) involved.

Financial and Residual Risk Criteria -When performing a business impact analysis (BIA), the process will include not only a specification of the maximum period that GCFL can go without the information processing services involved, it will also include analysis of the financial losses potentially incurred during the outage, a qualitative residual risk assessment and an asset criticality analysis.

Development

Business And Computer Continuity Planning - A standard organization-wide process for developing and maintaining both business contingency plans and computer contingency plans must be documented and maintained by Information Systems Department.

Reversion To Manual Procedures - If Group critical business activities could reasonably be performed with manual procedures rather than computers, a manual computer contingency plan must be developed, tested, periodically updated, and integrated into computer and communication system contingency plans.

Occupant Emergency Plan (OEP) - An Occupant Emergency Plan will be included as part of overall business continuity planning within Group. This plan will focus on personnel safety in the face of physical threats, which include, but are not limited to, exposure to hazardous materials (whether chemical or biological), sudden weather events (tornadoes, severe thunderstorms, etc.), bomb threats, violence at the workplace, and fires.

Testing

Contingency Plan Testing - To the extent practical and feasible, computer and communication system contingency plans must be tested at regular intervals to assure that they are still relevant and effective. Each such test must be followed by a brief report to top management detailing the results of the test and any remedial actions that need to be taken.

Telephone Number Testing - Each calendar quarter, Information Security Department staff must test and revise a call tree indicating every available telephone number for every worker involved in information-systems-related contingency planning, as well as disaster and emergency response.

Recovery and Restoration

The rights of restoration of critical / important data are with Only IT person. In case of emergency, details or procedure of such restoration can be explained to any other staff of origination (other than IT person).

R. Fire Safety Policy

Purpose

The purpose of this Fire Safety Policy is to eliminate the causes of fire, prevent loss of life and property by fire. It provides employees with information and guidelines that will assist them in recognizing, reporting, and controlling fire hazards.

Background

GCFL is committed to minimizing the threat of fire to employees, visitors, and property. GCFL complies with all applicable laws, regulations, codes, and good practices pertaining to fire prevention. GCFL's separate Emergency Action Plan spells out the procedures for responding to fires. This Fire Safety Policy serves to reduce the risk of fires at GCFL place in the following ways:

1. identifies materials that are potential fire hazards and their proper handling and storage procedures;
2. distinguishes potential ignition sources and the proper control procedures of those materials;
3. describes fire protection equipment and/or systems used to control fire hazards;
4. identifies persons responsible for maintaining the equipment and systems installed to prevent or control ignition of fires;
5. identifies persons responsible for the control and accumulation of flammable or combustible material;
6. describes good housekeeping procedures necessary to insure the control of accumulated flammable and combustible waste material and residues to avoid a fire emergency; and
7. provides training to employees with regard to fire hazards to which they may be exposed.

Assignment of Responsibility

Fire safety is everyone's responsibility. All employees should know how to prevent and respond to fires, and are responsible for adhering to GCFL policy regarding fire emergencies.

A. Management

Management determines the GCFL fire prevention and protection policies. Management will provide adequate controls to provide a safe workplace, and will provide adequate resources and training to its employees to encourage fire prevention and the safest possible response in the event of a fire emergency.

B. Plan Administrator

Responsible Person(s) shall manage the Fire Prevention Plan for the GCFL, and shall maintain all records pertaining to the plan. The Plan Administrator shall also:

1. Develop and administer the GCFL fire prevention training program.
2. Ensure that fire control equipment and systems are properly maintained.
3. Control fuel source hazards.
4. Conduct fire risk surveys and make recommendations.

C. Supervisors

Supervisors are responsible for ensuring that employees receive appropriate fire safety training, and for notifying Responsible Person when changes in operation increase the risk of fire. Supervisors are also responsible for enforcing GCFL fire prevention and protection policies.

D. Employees

All employees shall:

1. Complete all required training before working without supervision.
2. Conduct operations safely to limit the risk of fire.
3. Report potential fire hazards to their supervisors.
4. Follow fire emergency procedures.

Plan Implementation

A. Good Housekeeping

To limit the risk of fires, employees shall take the following precautions:

1. Minimize the storage of combustible materials.
2. Make sure that doors, hallways, stairs, and other exit routes are kept free of obstructions.
3. Dispose of combustible waste in covered, airtight, metal containers.
4. Use and store flammable materials in well-ventilated areas away from ignition sources.
5. Use only nonflammable cleaning products.
6. Keep incompatible (i.e., chemically reactive) substances away from each other.
7. Perform “hot work” (i.e., welding or working with an open flame or other ignition sources) in controlled and well-ventilated areas.

8. Keep equipment in good working order (i.e., inspect electrical wiring and appliances regularly and keep motors and machine tools free of dust and grease.)
9. Ensure that heating units are safeguarded.
10. Report all gas leaks immediately. Responsible Person shall ensure that all gas leaks are repaired immediately upon notification.
11. Repair and clean up flammable liquid leaks immediately.
12. Keep work areas free of dust, lint, sawdust, scraps, and similar material.
13. Do not rely on extension cords if wiring improvements are needed, and take care not to overload circuits with multiple pieces of equipment.
14. Ensure that required hot work permits are obtained.
15. Turn off electrical equipment when not in use.

B. Maintenance

Responsible Person(s) will ensure that equipment is maintained according to manufacturers' specifications. GCFL will also comply with requirements of the National Fire Protection Association (NFPA) codes for specific equipment. Only properly trained individuals shall perform maintenance work. The following equipment is subject to the maintenance, inspection, and testing procedures:

1. equipment installed to detect fuel leaks, control heating, and control pressurized systems;
2. portable fire extinguishers, automatic sprinkler systems, and fixed extinguishing systems;
3. detection systems for smoke, heat, or flame;
4. fire alarm systems; and
5. emergency backup systems and the equipment they support.

Training

Responsible Person shall present basic fire prevention training to all employees upon employment, and shall maintain documentation of the training, which includes:

1. this Fire Prevention Plan, including how it can be accessed;
2. good housekeeping practices;
3. proper response and notification in the event of a fire;
4. instruction on the use of portable fire extinguishers; and
5. recognition of potential fire hazards.

Supervisors shall train employees about the fire hazards associated with the specific materials and processes to which they are exposed, and will maintain documentation of the training. Employees will receive this training:

a. at their initial assignment;
b. annually; and
c. when changes in work processes necessitate additional training.

Smoking

Smoking is prohibited in all area of GCFL. Certain outdoor areas may also be designated as no smoking areas.

Program Review

Responsible Person shall review this Fire Safety Policy at least annually for necessary changes.

Fire Safety Do's and Don'ts

The following are what to do in case of a fire:

1. Acquaint yourself with the layout of the escape routes, staircases, refuge areas and the location of fire alarm.
2. Keep always closed the fire doors of staircases, main entrance to the factory building/ company.
3. All the fire protection installations such as fire pumps, wet riser-cum-downcomer, sprinkler installation, fire extinguishers etc should be kept in a good state. Timely use of these will help in controlling/extinguishing the fires in the early stages, thereby minimising life losses and property losses.
4. Always maintain good housekeeping.
5. Practice evacuation drills periodically.
6. Irrespective of the magnitude of fire, summon the Fire Brigade at the earliest.
7. Seek the advice and guidance of Fire Brigade Department in the matter of fire safety.
8. In case of fire, guide the Fire Brigade Department personnel about the location and extent of fire, information about trapped persons, if any, and provide any other information they may request. Help them to help you.
9. Remember, **THE FIREMAN IS YOUR FRIEND**.

The following are what not to do in case of a fire:

1. Do not allow storages or obstructions in the common corridors and staircases. These exit routes, if maintained clear, will help easy escape in case of fire.
2. Do not allow the Fire doors of the staircases to be kept open. In case of fire, heat and smoke enters the staircases and prevent the escape of people.
3. In case of fire, do not use LIFTS for escape. They may fail midway trapping people inside. Use only staircases.
4. Do not allow Electric Meter Rooms to be used as storages, dumping places or as living quarters for servants. They are potential fire hazards.
5. Never paint or coat fire detectors or sprinkler heads. If done, they will become ineffective.
6. Do not 'switch off' Fire/Smoke Detection System. This may lead to fire remaining unnoticed till it assumed large magnitude.

7. Do not 'switch off' electricity of the entire building in the event of a fire. This will cause stoppage of all the fire protection and fire fighting system installed in the building.
8. Do not carry out additions and alteration in the building. Consult Fire Brigade before undertaking such works.

Important Emergency Numbers

Below are some important numbers in case of emergency:

NATIONAL EMERGENCY NUMBER	112
POLICE	100
FIRE	101
AMBULANCE	102
WOMEN HELPLINE	1091

S. Visitor Policy

Purpose

In order to assure the safety and security of Company associates, its visitors, and its property and to insure that only authorized personnel have access to the Company facilities, the following policies have been adopted:

Policy & Procedure

Visitors:

2. All visitors must be sign in and out entry to the prescribed register maintained by the appropriate administrative associate or receptionist.
3. All the assets owned by the visitor like Laptop, mobile, which will be connected to Company network & used in office premises must be checked by the IT person.
4. Any access of data to be given to visitor after proper approval of management.
5. Before leaving office premises, IT person must delete all the possible data used by the visitor during work hours.

Suppliers, Contractors, Delivery Personnel

1. Vendors will use their Bill of Lading as an acceptable ID; however, such persons shall not be permitted outside their normal areas of pick-up and delivery without being escorted by an appropriate associate.
2. Delivery personnel (i.e., UPS, Federal Express, etc.) will be permitted to make their deliveries to the appropriate areas without a badge or pass, provided they do not go outside normal areas of pickup or delivery.

T. IT Committee:

Companies within the group must have IT Committee to review the IT Policies. Such IT Committee must consist persons from IT background. Such policies are periodically reviewed by

IT Committee. In case of any deficiency in policy must be resolved with appropriate time & circulated to all staff.

IT Committee must be formed by NBFC in group as per the direction given by RBI. Other companies in group can adopt the rule & procedure given by their respective authority or can adopt the rules & regulation given by RBI.

U. Patch Management Policy:

Objective:

Patch management policy is set of guidelines to ensure controlled, efficient and secure patching These guidelines contain steps and procedures that one should follow when patching bugs and vulnerabilities.

Identification and Procurement of Assets:

There are different types of patches - security patches, hotfixes, service packs, etc. that are required to be tested on all the hardware present in the office. Patch Update is undertaken by the IT person in their desktop regularly. Thereafter the Patch test is run on all the Computers on every alternate Saturdays (specifically on the Saturdays where the Employees have Holiday) and during Holidays.

In case of any patch failure, the solution is been sought by the IT personnel and the same is been reported to the Management. Accordingly upon the Management Approval, necessary steps are been taken by the IT Personnel.

Approval Authority: This policy shall be approved by the Board of Directors.

Review Policy: This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs.

V. Data Migration Policy:

Preamble:

GeeCee Fincap Limited ("the Company") is an Investment and Credit Company (ICC). The Company's primary activity is investing in securities, mobilization of Capital and lending. The Company is prone to inherent business risks like any other organization.

The Board of Directors ("Board") of the Company has adopted the Data Migration Policy ("This Policy") as per the Master Direction issued by RBI dated 7th November, 2023, which specifies a systematic process for data migration, ensuring data integrity, completeness and consistency. The policy shall, inter alia, contain provisions pertaining to signoffs from business users and application owners at each stage of migration, maintenance of audit trails, etc.

Scope & objective:

Data migration is the process of moving data between storage systems, applications, or formats. Typically a one-time process, it can include extracting, transforming and loading the data. A data migration project can be initiated for many reasons, such as upgrading databases, deploying a new application or switching to internal server.

The Company will identify the data migration scope by analysing the business needs, the data relevance, the data availability, and the data compatibility. The Company will prioritize the data migration scope by considering the value, the urgency, and the impact of the data. It can be defined by various criteria, such as business functions, data entities, data attributes, data quality, data dependencies, or data transformations need.

Types of Data Migration:

- Replacing or upgrading servers or storage equipment.
- Moving on-premises inhouse infrastructure.
- Performing infrastructure maintenance.
- Migrating applications or databases.
- Installing software upgrades.
- Moving data during a company merger or data centre relocation.

Process of Data Migration:

The data migration process requires organizations to prepare, extract and transform data and to follow a specified set plan -- which differs by organization and migration.

Data Backup:

The best practices of data migration dictate the creation of a full backup by IT department and software vendors of the content which the company plans to move before executing the actual migration. It will provide protection in the event of unexpected migration failures and data losses.

Post Migration Maintenance:

- Review Status and Complete Migration.
- Clean Up Migration Files.
- Troubleshoot the Migration Process.

Implementing Data Security and Privacy Measures:

The Company will ensure the confidentiality, integrity, and availability of data and data encryption will be a major priority before beginning the Data Migration procedure. Implementing robust encryption techniques, access controls, and data masking are essential to protect sensitive information during and after the migration process.

Signoffs from Business Users and Application owners with Audit Trail:

The Company will ensure the unit, system, online application, and batch application tests need to be carried out before the conversion can be signed off by the business users at each stage of migrations with audit trails.

Periodic Review:

The policy will be reviewed periodically or at the time of any major change in existing IT environment affecting policy and procedures and placed to the Board for approval. This policy will remain in force until next review / revision.

W. Framework on Recovery Point Objective & Recovery Time Objective:

Preamble:

GeeCee Fincap Limited ("the Company") is an Investment and Credit Company (ICC). The Company's primary activity is investing in securities, mobilization of Capital and lending. The Company is prone to inherent business risks like any other organization.

The Board of Directors ("Board") of the Company has adopted this framework as per the Master Direction issued by RBI dated 7th November, 2023, which specifying a suitable metrics for system performance, recovery and business resumption, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for all critical information systems and risk-based approach for non-critical informations.

Metrics for System Performance:

The best metrics for evaluating data system performance depend on the specific business needs. The Company used some commonly metrics include throughput, latency, availability, error rate, and scalability.

Recovery Point Objective:

The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system or network goes down as a result of a hardware, program or communications failure. The RPO is expressed backward in time -- that is, into the past -- from the instant at which the failure occurs and can be specified in seconds, minutes, hours, or days. It is an important consideration in a disaster recovery plan.

Once the RPO for a given computer, system or network has been defined, it determines the minimum frequency with which must be made. This, along with the recovery time objective. Businesses can choose to have any number of different tiers for an RPO based on workload and loss tolerance.

Critical Data / Infrastructure (2-4 HOURS):

For the most valuable data organizations can't afford to lose at all, such as banking transactions, the RPO needs to be set for continuous backup.

Semi Critical (1-4 HOURS):

For data that is semi critical, which could include data on file servers or chat logs, an RPO of up to 4 hours should be set.

Less Critical (4-12 HOURS):

Data such as marketing information is often deemed as less critical, for example, and can work with a longer loss tolerance with an RPO of up to 12 hours.

Infrequent (13 - 24 HOURS):

Infrequently updated data, such as product specifications, can have an RPO of up to 24 hours.

Recovery Time Objective:

The RTO comes into play after a loss event. It will help the Company to answer the question of how quickly they can recover after data loss due to a failure, natural disaster or malfeasance. RPO and RTO will work together in a time sequence, with RPO making sure a business has the right data backup policies in place and RTO ensuring it can recover data backups quickly.

Periodic Review:

This framework will be reviewed periodically or at the time of any major change in this framework and placed to the Board for approval. It will remain in force until next review / revision.