GEECEE FINCAP LIMITED

CYBER SECURITY POLICY
&
CYBER CRISIS MANAGEMENT PLAN

Effective Date	**30.03.2024**
1st Review	**04.02.2025**

OBJECTIVE:

The purpose of this policy is to Implement adequate usage controls towards the email facility and protect the Information Assets from various threats related to the usage of E-mails like viruses, spam mails, leakage of information through e-mails etc. To encourage an efficient communication system and to add value to the services offered. Implement adequate security controls to ensure that the vulnerabilities associated with email facility are minimized e.g. antivirus etc.

CONTROLS OVER E-MAIL ACCESS :

i. Access to the e-mail facility from the company should be given to only those users who have a business need.

ii. The users should be allowed to access their emails using the approved client email software only.
E.g. outlook;

iii. Each user should be held accountable for contents of his / her email. Each user must have a distinct and unique e-mail ID to help establish accountability.

iv. In case of any unusual activity like chain mails, spam emails, virus emails, etc. the user should report it to the IT Team.

v. Each employee should be responsible for the contents of his/her e-mail and all actions performed using his/her email login credentials.

vi. Email should be used only for business purposes. Personal or non-business use of the Systems is not permitted.

vii. Users should use only their own E-Mail account and should not allow anyone else to access their account. Users should identify themselves by their real name. Users should not represent themselves as another user. Each user should take precautions to prevent unauthorized use of the Email account.

viii. Users should not provide other unauthorized persons with their E-Mail ID and password.

ix. Users should not send confidential or restrictive information via E-mail, unless it is approved. E-mail should not he used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others. If any employee receives offensive E-mail/s, he / she may either communicate with the originator of the offensive E-mails, asking him/her to stop sending such messages, or report such offensive E-mails directly to the IT Team and Management.

x. Users should not post network or server configuration information about any devices to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.

xi. Users should not modify the security parameters within the E-Mail system.

xii. Users should not send unsolicited bulk mail messages. This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious E-Mail, including but not limited to "mail bombing," is prohibited.

RESTRICTION ON USE OF ANOTHER USER'S EMAIL ID: :

i. Users accessing the e-mail services must not use or access an e-mail account assigned to another individual to either send or receive messages.

ii. An approval from appropriate authority should be obtained in case a user's e-mail needs to be read in his / her absence.

iii. At times emails of some persons need to be accessed on an on-going basis by other/s, such facility should be used / allowed only for receiving or reading mails. For sending mails through that ID, prior approval shall be taken.

MAILS FROM UNKNOWN SOURCES:

Opening of e-mails and attachments from unknown or un-trusted source is strictly prohibited.

INCIDENT MANAGEMENT POLICY:

Objective:
The Incident Management Policy is designed to;

- Establish a process for identification and management of incidents, problems, malfunctions and abuses.
- Provide guidance to the technical and management users to enable quick, efficient and effective recovery from Incidents or problems.
- To minimize loss from Incidents or problems.

- To carry out a root cause analysis, document and learn from the Incidents or problems and implement controls to arrest recurrence of the Incidents or problems.

Policy Scope:
This policy is applicable to various information assets and to all users.

Policy Statement(s):

a) Identify possible Incidents and steps for recovery:
The **Incident response team (IRT)** should ensure that various possible incidents or problems are studied and documented including the steps for resolution. Each possible incident or problem along with the steps should be documented and reviewed and rehearsed at regular intervals. The document should be available with the IRT.

b) Training for Incident Identification:
Adequate and repeated training should be given to USERS to help them understand and identify an event / incident / problem. This would include demonstration of sirens, alarms, incorrect system behaviour, other indications etc.

c) Ensure Incident / Problem Reporting:
The users should be informed about the process of incident / problem reporting, to the appropriate authority for an early resolution. If any vulnerability is identified in the off-the-shelf products, it should be reported to the respective regulatory authorities for meeting the compliance requirements, wherever applicable.

d) Analyse the Incident / Problem:
Incidents / Problems should be assigned appropriate severity level. As part of incident / problem analysis, incident / problem severity levels should be determined by relevant designated staff members/asset custodians.
These USERS should be trained to discern incidents / problems of high severity level. Moreover, criteria used for assessing severity levels of incidents / problems should be established and documented.

e) Contain the Incident / Problem and remove the cause:
The Incident Response Team should first try to contain the Incident / Problem to ensure that the damages are minimal.
After containment the Incident Response Team should remove the cause of the Incident / Problem. The Team should be careful to safeguard the evidences to help the investigation. The Team should monitor all the incidents / problems and ensure that the timelines for resolution are achieved.

f) Escalation Process should be established:
Timeframe for resolution of Incidents / Problems should be commensurate with the severity level and corresponding escalation process should be defined to ensure timely resolution. These escalation procedures should be tested at regular intervals to evaluate effectiveness.

If an Incident / Problem is likely to develop in a major crisis, senior management should be immediately informed. Thereafter, senior management should take a call about declaring disaster and taking necessary actions thereof. Intimation about such cases should also be given to customers or relevant statutory authorities if applicable. The employees / contractors and other relevant parties should not make comments or should not give any information about the incident on social media. Information to public will be given by Public Relations / Corporate Communications Department, if exists or by top management. In case of breach of regulatory requirements, legal and compliance team will take necessary action to report such incident / breach to the concerned authority.

g) Root Cause and Impact Analysis should be done:

The Incident Response Team should carry out a root cause analysis of the Incident / Problem to establish the reasons of incident / problem and document the findings.

Root Cause Analysis should cover the following:

a. Root Cause Analysis

- When did it happen?
- Where did it happen?
- Why and how did the incident / problem happen?
- How often had a similar incident / problem occurred over the last 3 years?
- What lessons were learnt from this incident / problem?

b. Impact Analysis

- Extent, duration or scope of the incident / problem including information on the systems, resources, customers that were affected;
- Magnitude of the incident / problem including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; and
- Breach of regulatory requirements and conditions, if any, as a result of the incident / problem.

c. Correction and Corrective Measures

- Immediate correction to be taken to address consequences of the incident / problem. Priority should be placed on addressing customers' concerns and / or compensation;
- Measures to address the root cause of the incident / problem; and
- Measures to prevent similar or related incidents / problems from occurring.

The root cause analysis will help identify the control weaknesses in technology and processes.

h) Implement additional / change of controls:
The IRT will review the root cause analysis and the weaknesses and define changes (including additional controls) to the technical and / or procedural controls to ensure against recurrence of such incidents / problems

VIRUS AND OTHER CONTROLS:

All incoming and outgoing mails should be subjected to scanning for viruses and content filtering.

RIGHT TO REVIEW E-MAIL CONTENTS

i. No email, automatic or otherwise, should be forwarded to personal or another user official and public email account unless required by business

i. Controls over sending critical information through emails

ii. Highly critical and confidential information like passwords, etc. should not be sent through normal email facility. Any other confidential documents sent by email should be password protected and the password should be communicated to the recipient in a secure manner.

MAIL SIZE AND MAILBOX RESTRICTIONS:

Maximum allowed mail size and inbox is mentioned below:
Max Mail Size - 5GB (In cloud)

Different Users have different mail size depending upon the Management Level.

BACKUP OF EMAILS:

i. The IT Department should ensure that adequate backups of emails on the server are taken.

i. In case a user needs to backup his / her emails for valid business reasons, the IT department should organize the backup, after obtaining appropriate approval from the requestor's manager.

ACCESS TO EMAILS FROM OUTSIDE:

Access to Emails from outside should be granted only against appropriate approvals from the user's manager.

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.

****