E-MAIL MANAGEMENT POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/EM/POL /011	1-Mar-2019	Initial version created	K. Gokhul	S.Nandhini
1.0	SQFT/EM/POL /011	1-Mar-2020	Reviewed and no changes done	K. Gokhul	S.Nandhini
1.0	SQFT/EM/POL /011	1-Mar-2021	Reviewed and no changes done	K. Gokhul	S.Nandhini
1.0	SQFT/EM/POL /011	1-Mar-2022	Reviewed and no changes done	K. Gokhul	S.Nandhini
1.1	SQFT/EM/POL /011	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/EM/POL /011	1-Mar-2023	Reviewed and no changes done	K. Gokhul	S.Nandhini
1.1	SQFT/EM/POL /011	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K. Gokhul

TABLE OF CONTENTS

1 PURPOSE

Exchange of information through electronic channels has become an absolute necessity for any individual or organization. At the same time, Exchange of business information through electronic media requires high levels of confidentiality and message integrity. The non-availability of such facilities even for a shorter period could severely hamper effective business activities of any organization in a big way. Information conveyed through electronic channels like fax and e-mail are considered as authentic information and decisions are being taken based on such messages and conveyed through the same channel. Besides, in many countries, information conveyed through electronic media is considered as legal document and accepted as evidence in courts of law.

This document provides the baselines and guidelines for securing information transferred through electronic mails.

2 SCOPE

This Policy applies to all users who have been authorized to use the e-mail facility of SQFT KS.

3 POLICY ELEMENTS

3.1 E-MAIL ACCOUNTS

- E-mail id should be created based on a consistent naming standard.
- Name and the initials shall be used for creating of a unique user id. (For e.g. a user). The mail id shall be based on the domain id allotted for the user.
- Common email IDs (For e.g. helpdesk@sqftks.com) should be provided for function-based activities for convenience of operations. This account should not be linked to the personal email id of members of the application group.
- External parties working for SQFT KS can have email IDs after approval. These email IDs should be differentiated from the employee IDs and will be allotted to a restricted group.
- For common mail ID, the request for new id must be approved.
- The creation of common-id must be approved by the office. These mail ids will be allotted to identify members of a group with adequate security measures.
- In general, all email accounts should be deleted immediately after the employee / consultant leaves SQFT KS. This practice is to prevent unauthorized access by the user and to protect the information exchange / leakage when he leaves the employment. This could be attributable to other reasons including consultant completing the assignment or application being phased out.
- However, based on business requirements, mail accounts of employees who have left the organization can be retained for a definite period with the approval of the head of the department. In such cases, the successor / supervisor shall be in-charge of the mails received in that mail id. Sending mails from that mail id is not allowed.

- HR is responsible for terminating the email accounts.
- All user mailboxes should be protected by password.
- Email users should set and protect their password in a secure manner as per password policy and Policys.
- The size of individual user mailbox should be restricted depending on the business requirement and level of usage.
- The e-mail administrator, with the approval of IT TEAM head reserves the right to reduce the mail box size of any mail user.
- The mail-id of any user can be blocked due to prolonged absence of the employee, observed misuse etc. This action will be taken in concurrence with the respective department head of the employee.

3.2 EMAIL USAGE

- Users owning the email account should be fully responsible for the content of email originated, replied or forwarded from their account to other users inside or outside SQFT KS.
- SQFT KS is in no way responsible for the content of the email, be it body of mail or the attachment.
- User should not send emails with any libelous, defamatory, offensive, racist or obscene remarks.
- Users should not send e-mails which is likely to contain virus or unsolicited mail (SPAM).
- Users should not use SQFT KS email systems to send chain mails for charitable fund raising campaigns, political advocacy efforts, religious efforts, private business activities or personal amusement and entertainment.
- The email system should not be used to copy and/or transmit any document, software or other information protected by copyright or any other law.
- SQFT KS could take appropriate disciplinary action in case of misuse of the e-mail system is found.
- The e-mail id of SQFT KS domain will be used only for official purposes. The e-mail administrator reserves the right to block any external mail-id or domain, from the mail-id of a particular user or a group of users or the entire domain without the prior approval to the user.
- If required, the user may request the e-mail administrator to release the site with reasons.
- Users should use disclaimer at the end of the e-mail.
- The following disclaimer can be used:

- "Information transmitted by this e-mail may be confidential and privileged and is intended for use only by the individual or entity to which it is addressed. If you are not the intended recipient or it appears that this mail has been forwarded to you without proper authority, you are not authorized to access, read, disclose, copy, use or otherwise deal with it and such actions may be unlawful. Internet communications cannot be guaranteed to be secured or error-free as information could be intercepted, corrupted, lost, arrive late or contain viruses. SQFT KS Technologies Limited therefore does not accept liability for any errors, omissions, viruses or computer problems experienced as a result of this transmission. Notice is hereby given that no representation, contract or other binding obligation shall be created by this e-mail."
- If the user is storing mails locally, the local mail files should be locked with a password. To prevent computer viruses, employees must not open attachments from an unknown source.
- For common mail id used by functional departments, the department concerned will allot an owner for the mail id. The owner has the authority and responsibility towards allocation of users for that mail id and sharing the password within the authorized group. Function level risk analysis will be carried out before the allotment of the mail id.
- The users of common mail ids will understand the risks associated with the common ids and will maintain the integrity and confidentiality of the information handled through the mail ids.
- The common mail ids will be used exclusively for the particular/associate functions for which the id has been allotted.
- Password for common mail id will be generated only by the owner and circulated to all members.
- Individuals accessing the e-mail services of SQFT KS Group must not use or access an e-mail account assigned to another individual to either send or receive messages. If there is a need to read another person's e-mail (while he /she are away on vacation for instance), message forwarding and other facilities must be used instead. A written approval from the COO must be obtained in case a user's e-mail needs to be read in his / her absence.
- Blanket forwarding of e-mail messages, Greetings, Graphics is prohibited.
- Users must regularly move important information from e-mail message files to word processing documents, text files, databases and other files. E-mail systems is not intended for the archival storage of important information as stored e-mail messages may be periodically expunged by systems administrators, mistakenly erased by users and otherwise lost when system problems occur.
- Users should be made aware of archiving old e-mails from their desktops.
- Users should promptly report all suspected security vulnerabilities or problems that they notice with the email system to the central support team.
- COO and Internal Audit have the authority to intercept, disclose, or assist in intercepting or disclosing e-mail communications in case of investigating a suspected violation.

- If absolutely required, IT TEAM can be asked to intercept e-mails only with the approval of the COO or Chairperson of the Information Security Steering Committee.

3.3 INCIDENTAL DISCLOSURE

For the central support team to intercept or disclose e-mail communications incase of investigating a suspected violation will require the approval from COO or the Chairperson of the Information Security and Privacy Steering Committee before initiating any of these activities.

Email forwarding should be used if users need other staff to check their mail. E.g. Manager forwarding his/her mail to secretary.

Private information like password, account number and PIN should not be sent by email. Use digital signatures or encryption for sending private information by e-mails.

3.4 BACKUP AND REDUNDANCY

E-mail administrators should be responsible for the backup of the e-mails.
Testing of recovery should be done every one year. Recovery needs to be tested by restoring backup files on the standby system

4 EXECUTIVE OWNER

Chief Operating Officer will be the executive owner of the Policy.
The Policy shall be approved by the Information Security and Privacy Steering Committee after review by the respective Department Heads and Chief Operating Officer.
The Chief Operating Officer, IT Head and users shall be responsible for implementing and executing the Policy's and guidelines mentioned in this document.
The records relating to this Policy shall be maintained by the IT Implementation Team member.
The implementation shall be monitored and reviewed by the Chief Operating Officer.

5 ROLES AND RESPONSIBILITIES

Abbreviations

P – Primary Responsibility

- - Cooperative Responsibility

N/A - Not Applicable

Responsibility

S.No	Activity	IT Team	COO	Department Heads	Users / Groups / Departments
1	Approval of new e-mail accounts	N/A	N/A	P	•
2	Creation of e-mail account and allotment of mail box	P	N/A	N/A	•
3	Server Maintenance and backup	P	N/A	N/A	•
4	Legal and proper use of e-mails	•	N/A	N/A	P
5	E-mail messages	N/A	N/A	•	P
6	Monitoring and Review of e-mail Policys	•	P	N/A	N/A
7	Backup of personal mail folder files	•	N/A	N/A	P

6 DEFINITIONS

COO	Chief Operating Officer
ISPSC	Information Security and Privacy Steering Committee
IPSO	Department Information and Privacy Security Officer
IT Team	Information Technology Team
Head	Group/Department Head

7 ASSOCIATED DOCUMENT

- E-Mail Management Procedure(SQFT/EM/PRO/011)

8 DOCUMENT MAINTENANCE

- Chief Operating Officer shall be responsible for document control and any changes.
- Updates shall be discussed by the COO and the head of the department.
- COO shall forward the document to Information Security Steering Committee for approval, after review.

End of Document