**E-Mail Security Policy and Procedure**

Doc ID: POL/0.1

Document Classification: Internal

July 2022

**Document Control Information**

| Document Name | E-mail Security Policy and Procedure |
| --- | --- |
| Document ID | POL/0.1 |
| Document Owner | Information Security Officer |
| Classification | Internal |
| Approved By |  |

| **Authorization** | | | |
| --- | --- | --- | --- |
| **Stakeholders** | **Read Access** | **Write Access** | **Media Type** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| **Amendment Log** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Author (s)** | **Reviewed By** | **Approved by** | **Brief description of the change** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**TABLE OF CONTENTS**

1.0 Purpose 4

2.0 Scope 4

3.0 Policy 4

3.1 Access to E-Mail 4

3.2 E-mail Access 4

3.3 Email Use 5

3.4 Awareness and Undertaking 5

3.5 Webmail Access 5

3.6 Legal Risks 5

3.7 Deactivation of E-Mail Access 6

3.8 E-Mail Clauses Reserved by {Company} 6

3.9 Transmission of Sensitive Information 7

3.10 E-mail Signature 7

3.11 E-mail Safeguards 7

3.12 Distribution List Management 7

3.13 Mailbox and E-Mail Size Limitations 7

3.14 Logging and Auditing 7

4.0 Procedure 8

4.1 E-mail Access Control 8

4.1.1 New E-mail account creation process 8

4.1.2 Change in E-mail ID 8

4.1.3 E-mail Deletion process 8

4.2 E-mail ID Management 8

4.3 Encrypting Restricted / Confidential Information 9

4.3.1 Using Microsoft Office Applications 9

5.0 Reference Documents 9

# Purpose

Electronic mail is a business resource and it is important to use it responsibly and implement adequate controls to ensure security and restrict its abuse.

E-mail security breach is becoming an increasingly significant threat to organizations around the world. While {Company} appropriate has security measures and controls that need to be a high level of vigilance as e-mail is rapidly becoming the principal means of business communication. This policy aims at laying down rules and best practices for e-mail usages both inbound and outbound.

# Scope

This policy applies to all users of {Company} and any such persons using the e-mail resources of the group.

# Policy

## Access to E-Mail

* E-mail should only be used for business purposes.
* All users must have a unique e-mail id, and it must not be shared between multiple people.
* Employees of {Company} must not use or access an e-mail account assigned to another individual. If there is a need to read another person’s e-mail while he / she is away, message forwarding and other facilities like delegate permission must be used instead. Written approval from the concerned Department Head, Management Representative and Head – HR must be obtained in case a user’s e-mail needs to be read in his / her absence. Such a facility should be used only for receiving and reading emails, not for sending mails.
* All messages sent using the company e-mail account are subject to logging and examination without any prior notice to the employees.
* Users should not automatically forward their e-mails to any address outside the group / company networks. Users will be responsible for mails forwarded to external parties. Employees found forwarding company data and/or confidential material to unauthorised third parties or outside the {Company} will face action as per the disciplinary action defined in the ISMS Policy.
* Webmail access shall be given by default to all the employees.

## E-mail Access

* The e-mail systems are intended for use in the conduct of {Company}’s business. All e-mail messages will be considered as {Company} records. The company retains all rights to read the contents of any message sent / received from the {Company} network.
* All emails are {Company} 's property.

## Email Use

* Unauthorized use of e-mail includes, but is not limited to:
  + Transmitting or storing offensive material like pornography and sexual harassment material.
  + Soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the user’s employment and the user’s responsibilities to {Company}.
  + “Spamming”, sending unsolicited messages, product promotions, sending or forwarding chain letters.
  + ‘Letter bombing’ (re-sending the same e-mail repeatedly to one or more recipients)
  + Creating, sending, receiving or storing materials that infringe the copyright or other intellectual property right of any third parties.
  + Sending, transmitting or distributing proprietary information, data or other restricted {Company} information.
  + Illegal content inserts threatening messages to individual or government or private entities.
* Personal Use:
* Using a reasonable amount of {Company} resources for personal e-mails is acceptable, but non-work related e-mail shall be saved in a separate folder from work-related e-mail. {Company} 's email system is strictly for business purposes only. Also, sending chain letters, junk mail, jokes and executables is strictly prohibited.
* All messages distributed via the company’s e-mail system are the company’s property.

## Awareness and Undertaking

* It is the responsibility of the users who have been provided with the e-mail facility to make themselves aware of the usage norms and their responsibilities towards it.
* Each employee who has been provided with the facility will have to sign the Acceptable Usage policy document indicating that he/she has understood and is bound by the usage norms.
* External users such as consultants and contract employees using the {Company} e-mail facility are also required to read, understand the usage norms and their responsibilities and sign the acceptable usage policy.

## Webmail Access

* Access to e-mail outside the premises through webmail will be provided by default to all the employees. The employees are encouraged to use webmail for remote e-mail.

## Legal Risks

* By following the guidelines in this policy, the e-mail user can minimize the legal risks involved in the use of e-mail.
* If any user disregards the rules set out in this Electronic Mail Security Policy, the user will be fully liable and {Company} can disassociate itself from the user as far as legally possible.

## Deactivation of E-Mail Access

* The e-mail ID of the person leaving the company will be immediately deactivated for outgoing mail once he / she leaves the organization.
* If the project / department requires the e-mail account to be active, the project / department will inform the HR team who in turn will inform the IT team. IT Team will then create a service desk ticket to convert the user’s mailbox as a shared mailbox.
* Delivery Head / Department Head will nominate a person who will get access for that shared mailbox and the same will be mentioned in the service desk ticket.
* The nominated person will get access for the resigned user’s mailbox.
* The Corporate account will be disabled immediately and deleted in a month’s time.
* The account deletion will not affect the e-mail address of the resigned user’s mailbox. Request to remove the access for the concerned person’s mailbox is generally done through service desk ticket.

## E-Mail Clauses Reserved by {Company}

* {Company} provides the corporate e-mailing facility to all users for official and business usage. Employees are required to send mails using official e-mail facility provided.
* {Company} reserves the right to inspect and review any data maintained in its e-mail system without the prior consent of or notification to the employee.
* {Company} may disclose contents of e-mail either internally or to external parties (law enforcement parties), as deemed fit by the organization.
* The personnel administering the e-mail system or any other individual will not be permitted to read an individual’s e-mail without the individual’s permission or without explicit authorization from the management.
* Auto forwarding of any e-mails containing {Company} data to any Internet-based accounts is not permitted. Only the following automatic responses are allowed to the Internet:
  + NDR messages (non-deliverable reports)
  + OOF messages (Out of Office)
  + Automatic response message
  + Delivery reports
* All messages sent and received by employees via e-mail are the sole property of {Company}
* At any time without prior notice, the management reserves the right to examine e-mails, personal files, directories, and other information stored on company-provided devices /equipment. This includes but is not restricted to desktops, laptops, handheld devices, portable pen drives, etc.
* {Company} may also disclose e-mail messages to law enforcement officials without prior notice to the employees who may have sent or received such messages.
* Hence users should restrict their communications to business matters in recognition of this electronic monitoring.
* The monitoring of mails should be done only by a group authorized to do so.

## Transmission of Sensitive Information

* Sensitive information will not be forwarded via any means unless that e-mail is critical to business and is encrypted (password-protection on document level in office documents / 7-Zip.

## E-mail Signature

* E-mail signatures should be according to the standards set by the organization. Users must not employ a scanned version of a hand-rendered signature, as the same could be misused by another person.

## E-mail Safeguards

* All e-mail attachments must be scanned for viruses before opening them.
* Users should not open e-mail attachments unless they are sure about its contents and know their senders.
* Users should not click on the "unsubscribe" link in the emails that they have received without subscribing to them. By doing this, spammer might get the information of the e-mail ID being 'live'.
* If users receive an email from unknown and/or un-trusted source, it might be spam or a phishing email. All such emails need to be forwarded to [reportphish@rediff-inc.com](about:blank) so that they may be blocked.
* The following file types are blocked by our anti-virus system:
  + ADE;ADP;BAS;BAT;CHM;CMD;COM;CPL;CRT;EXE;HLP;HTA;INF;INS;ISP;JS;JSE;LNK;MDB;MDE;MSC;MSI;MSP;MST;PCD;PIF;REG;SCR;SCT;SHS;URL;VB;VBE;VBS;WSC;WSF;WSH
* The above file types are blocked as they are frequently used in virus mails. This is a secondary measure that will protect the system in case the virus scanner is not able to catch a potential new virus. The attachments that are blocked are not saved.

## Distribution List Management

* Mails to a larger group must always be sent using the group lists and by authorized and select few individuals only.
* Only group owners must have the right to authorize additions and deletions to the group lists.
* Mass mailing like “New Year” or any other festival greetings should be discouraged.
* Unsolicited emails unless they have reasonable justification and approval are prohibited by the company’s email policy.

## Mailbox and E-Mail Size Limitations

* Forwarding large files to multiple recipients may congest networks or mail systems of both source and target systems. The user should, therefore forward only relevant official messages/data.

## Logging and Auditing

* E-mail messaging logs must be captured by the email administrator.
* Logging of activity on {Company} equipment is limited and restricted, and this logging will only be used to troubleshoot technology problems and to capture data to provide proof of illegal outside (external to {Company}) activity. Capturing of data from internally identifiable computers will only be done after approval from HR / Legal.

# Procedure

## E-mail Access Control

## New E-mail account creation process

* Employee Account Creation Process is as follows:
  + Details of the employee for whom email ID is to be created shall be filled up in the MIS by HR Team and forwarded to the IT Team
  + The request received for the creation of email ID must be approved by the respective Department Head / Delivery Head
  + The IT Team creates the email ID for the new joinee.Creation of e-mail id is communicated back to the HR .

## Change in E-mail ID

* It must be ensured that employee email account is created based on the nomenclature followed for e-mail ID creation, except in exceptional circumstances where two persons share the same name.

Incase where a user requests for a change in e-mail ID for a reason of change in his name (marriage in case of females or other reasons), the Account changes process is followed:

* Details of the employee for whom the changes in the email ID is to be performed shall be filled up in MIS by HR and forwarded to the IT team
* The IT team renames the email ID of the employee. The existing e-mail ID becomes an alias to the renamed email ID.
* The changes are then communicated back to the HR.

## E-mail Deletion process

* Employee account deletion process is as follows:
  + Details of the employee for whom the deletion of the email ID is to be performed shall be filled up in MIS by HR and forwarded to the IT team
  + The IT team suspends / deletes the email ID of the employee. The password of the email ID is changed immediately
  + The deletion of the email ID is then communicated back to the HR / Department Head.
  + Outgoing mail should be barred on the last working day. All such email accounts must be disabled for login at the end of the last day so that the employees will not be able to access their emails after their last day within {Company}

## E-mail ID Management

* Employees may have personal and/or group ID
* The e-mail id must follow a standard nomenclature as mentioned below:
  + <first name><second name initial>@entityname.com
* In case, there are two people with the same name, the nomenclature should be:
  + <first name><second name initial>.<last name> @ entityname.com
* The distribution e-mail id must follow a standard nomenclature as mentioned below:
  + <group name> @ entityname.com

## Encrypting Restricted / Confidential Information

## Using Microsoft Office Applications

* Most Microsoft Office applications provide a reasonable level of encryption by password protecting office documents.
* Whenever a word document or an excel sheet needs to be sent over an e-mail and the content is of sensitive / confidential nature, password protection option should be used.
* The user needs to ensure that the password is in-line with the password guidelines set in the Logical Access Control Policy to thwart password guessing / brute-forcing attempts.
* To password protect word document, select the “File” menu and click “Protect Document” and select the “Encrypt with password” option.

# Reference Documents

* ISMS Overview Policy
* ISO 27001:2013
* Statement of Applicability for ISO27001:2013
* Acceptable Usage Policy
* Logical Access Control Policy