Information Security Management System
Email Security Policy & Procedure

Document no. JMBGRP/ISMS/Pol-ES

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document to ensure secure email access, maintenance and secure handling of emails.	
Custodian	Corporate IT dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT Dept.	

Distribution list

Name
To all locations of JMB group.

Version History

Version no.	**Version date**	**Approved by**	**Comments**	**Signature**
v1.0	28.08.2018	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	10.01.2019	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	08.02.2020	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	11.02.2021	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.1	25.03.2022	Manish Jaiswal (Group CTO)	Logo changes done in this policy	
v1.2	18.08.2023	Manish Jaiswal (Group CTO)	Document reviewed. Modification done to "13. Reference to ISO 27001:2022	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "Procedure, Exceptions , Disclaimer"	

Contents

Purpose

JMBGRP has provided Electronic Mail to facilitate business communication and productivity amongst its employees and business associates. In order to ensure that electronic mail meets it desired objective, adequate and sufficient care has been taken by JMBGRP to provide a safe and secure infrastructure to the users. However equal responsibility rests with employees as well to ensure that, on no account, their individual or collective actions impacts electronic communication in any manner.

The policy and procedure on electronic mail seeks to articulate these principles and elaborates various aspects so that employees understand the purpose of electronic mail communication in spirit and intent.

Scope

The policy document is applicable to:

- All Locations of J. M Baxi Group in India
- All Employees of J. M Baxi Group

Policy Statement

- The Email system given to employees is an asset of JMBGRP and has been provided to the employees to improve business communication and contribute to the productivity of the company.
- Email service is one of the critical business value chain components in today's business and it shall be the endeavor of every employee to use it in a responsible manner.
- In order to ensure efficient usage of the Email service the company has established adequate and sufficient infrastructure along security controls and processed to facilitate internal and external exchange of communication between employees, third parties and business associates.
- There shall be formal provisioning and a de-provisioning process for all employees.
- For access of mails on mobile phones, tablets, the employee shall go through a dedicated provisioning and a de-provisioning process.
- The e-Mail Security Policy outlines the procedure, controls and responsibilities for ensuring that JMBGRP's e-Mail system is not misused and serves as an efficient mode of business communication.
- JMBGRP shall reserve the rights to inspect any mail for its contents should circumstances warrant such an action.
- For any usage of the E Mail service as provided for business, which will result in an undesirable harmful business impact, erosion of customer trust, impact brand and shareholder value; but not restricted to the mentioned inclusions shall be liable for disciplinary or even legal action.

- JMBGRP does not permit usage of public mails for business communication under any circumstances and any violation in this regard meet with a disciplinary action.

Procedure

1.1. This procedure on E Mail shall address the following areas as listed under

1.1.1. Email ID Creation

1.1.2. Client Hardware & Software

1.1.3. Mailbox Size

1.1.4. Email Size

1.1.5. Mail Storage

1.1.6. Automatic Forwarding/ Delegation of e-mail [To alternate Address]:

1.1.7. Maintenance

1.1.8. Use of E-Mail:

1.1.9. Monitoring e-mail Use

1.1.10. E Mail on Mobile Devices

1.1.11. E Mail Account Deletion & Mail Retention Process

1.1.12. Information Handling

1.1.13. Personal Use and Security

1.1.14. Critical Information

1.1.15. Special Precautions to employees when sending External e-Mails:

1.1.16. E-mail Etiquette

1.1.17. Other Good Practices

1.1.18. Disclaimer

1.2. **E-mail ID creation**

1.2.1. All e-Mail IDs shall be centrally registered by the IT Team on receipt of appropriate approval from the HOD.

1.2.2. For new employees this process shall be completed at the time of induction.

1.2.3. Users shall be informed of their User ID and password by the IT service desk. Users need to change their password immediately after getting the ID (the user will be asked to change their e-mail password when they log on for the first time).

1.2.4. The user shall be the owner of his/her e-Mail ID and shall be solely responsible for any use of the e-Mail ID allotted.

1.2.5. All e-Mail accounts maintained on the company's e-Mail systems are property of the company.

1.2.6. No user shall have more than one E-Mail ID depending as per business requirement and based on approval from the HOD.

1.2.7. Users must maintain the confidentiality of their passwords and accounts and will be held responsible for any unauthorized use their account.

1.2.8. Users shall maintain strong passwords as per the password policy.

1.3. Client Hardware & Software

1.3.1. In general, employees shall only use designated desktops and laptops issued to them for accessing e-Mails. In case of travel, while using web access employees may use personal laptops or other unmanaged devices , but shall refrain from opening attachments. Usage of Persnal Devices/ Un-managed Devices shall be done with abundant caution as they may have key loggers which will track all the information entered by the users.

1.3.2. The company provides a standard E Mail platform, and no other mail application shall be permitted. The only exception to this shall be in case of users who use smart phones and tablets.

1.4. Mailbox size:

1.4.1. The mailbox size for each user shall be restricted to 1 TB as maximum limit.

1.4.2. Mailbox with 30GB for all shall be provided.

1.4.3. Mailbox size with more than permitted size shall be managed through the exception process with a definite expiry date.

1.4.4. The system shall flash a warning message when a user’s mailbox size approaches the maximum limit.

1.5. E-mail size:

1.5.1. The size of an e-mail that a user can send / receive shall be restricted to 25MB as the maximum limit.

1.5.2. Any user who wishes to send / receive e-mails, which are larger than the specified 25MB, shall obtain approval from his HOD stating the business requirement, upon which the size can be increased.

1.5.3. The decision to maintain higher than normal mail inbox and outbox size shall be based on the approval from the concerned HOD and the IT.

1.5.4. The E-Mail Administrator shall increase the maximum limit and inform the IT Team and HOD.

1.5.5. If the increase in the mailbox size is for a specific duration then the same shall be revoked upon the expiry of the request.

1.6. **Mail Storage**

1.6.1. Limits shall be applied to mailbox sizes 30 GB and users shall maintain mailbox size by periodically archiving and deleting unwanted mails.

1.7. **Automatic Forwarding/ Delegation of e-mail [To alternate Address]:**

1.7.1. The automatic e-mail forward facility/ delegation facility shall not be made available to users.

1.7.2. Users shall also not have the rights to create other rules as available on the mail platform.

1.7.3. Any user who wishes to activate automatic forwarding facility/ delegation facility, shall request his HOD for the same. The request shall contain the reason and the period for which the facility is required.

1.7.4. After approval from the HOD, the IT Administrator/IT Team shall activate the automatic forwarding facility/ delegation facility and inform the HOD and user, Location IT Manager and IT–Head.

1.7.5. The System Administrator shall deactivate the automatic forwarding facility when the period for which the facility required has expired.

1.7.6. The System Administrator shall maintain a list of all the users who have enabled automatic forwarding and delegation facility on their mailboxes.

1.7.7. A list of users who have availed this facility, shall be submitted on a quarterly basis to Head – IT, HOD and Location IT Manager.

1.8. **Maintenance**

1.8.1. Users should delete any e-Mail messages that are not needed and set the e-Mail client to automatically empty the 'Trash' in 30 days.

1.8.2. E-Mail accounts shall be locked after 90 days if not in use and deleted when it has been confirmed the user has left the organization. Messages shall be archived up to 90 days after deletion.

1.9. **Use of E-Mail:**

1.9.1. E-Mail facilities are provided by the company to employees and other stakeholders for the organization's business purposes.

1.9.2. The following is not permitted in e-Mails:

1.9.2.1. Sending or forwarding e-Mails containing libelous, defamatory, obscene or pornographic material or derogatory remarks regarding race, religion, colour, nationality, marital status, age, physical disability, mental disability, medical condition or sexual orientation etc. If a user gets information about any other person using e-Mail for any of the above purposes they should notify their Manager or the IT Help Desk.

1.9.2.2. Sending or forwarding chain e-Mails, humorous pictures/videos.

1.9.2.3. Forwarding external virus warning messages to other users (these are usually hoaxes). If one is not sure whether a virus warning is genuine or a hoax, send it to the IT Service Desk for advice.

1.9.2.4. Spoofing or attempting to spoof e-Mail addresses.

1.9.2.5. Sending e-Mail messages using another person's e-Mail account without permission.

1.9.2.6. Copying or forwarding a message or attachment containing proprietary information of the originator or one that can attract copyright violations.

1.9.2.7. Disguising or attempting to disguise one's identity when sending mail.

1.9.2.8. Using Internet-based mail services such as Yahoo/Hotmail/Rediff mail etc. to transmit any sensitive company information.

1.9.2.9. Circulation of chain mails.

1.10. **Monitoring e-mail Use**

1.10.1. The organization reserves the right to monitor e-Mails without further notification. Such monitoring shall be conducted in accordance with company policies and national laws.

1.10.2. The organization may block incoming mail or revoke e-Mail IDs that violate policies of the company or laws of the land.

1.10.3. Non-Compliance to the requirements set out in this policy shall attract disciplinary action. Evidence of such non-compliance shall be collected in order to initiate any disciplinary action.

1.11. **E Mail on Mobile Devices**

1.11.1. Mobile devices such as Apple and Android are permitted to be used to access emails based on the business HOD or Security In-charge approvals.

1.11.2. On all android devices only those mail applications as approved by IT shall be configured.

1.11.3. All security settings shall be configured by IT for mobile devices and shall be handed over to the user.

1.11.4. Users shall not be allowed to detach attachments and store them on a local folder.

1.11.5. Users shall not be allowed to forward mails to public mail accounts as the content manager tool deployed shall block the same.

1.11.6. Mail Signature and Disclaimer as permitted by JMBGRP shall be displayed on all mails.

1.11.7. By design IT Team shall be kept in CC for the emails.

1.11.8. BCC shall be blocked.

1.11.9. Mails on mobile devices shall be monitored.

1.12. E Mail Account Deletion & Mail Retention Process

1.12.1. When the employee has resigned, has been terminated or has been transferred then upon instruction from HR and ratified by the concerned HOD, IT Team shall initiate with the account removal process. Once done IT Team shall inform the concerned HOD, HR Department and Location IT team where ever applicable.

1.12.2. The emails of outgoing employees will be retained for one year by the IT team, based on written instructions from the Head of Department (HOD) or business requirements. After this period, the emails will be securely destroyed unless retention is required due to legal or regulatory reasons. During the retention period, the emails will be stored securely and will not be accessed by the IT team.

1.12.3. If any of the mails from the outgoing employee are to be forwarded or be accessed by the new incumbent or the HOD, then it shall be done through a request to IT clearly stating the reason, business requirement and the duration for which the mails need to be accessed.

Personal Use and Security

1.12.4. Users are allowed to use e-Mail occasionally for personal communication, but prolonged or frequent use of e-Mail for personal reasons is not permitted and may result in disciplinary or even legal action.

1.13. Critical Information

1.13.1. Employees shall send critical information by e-Mail after securing the content with encryption and protecting it with a password. E.g. using WinZip or setting a password in Microsoft Word or Excel file while saving the file. Communication of the password to the recipient shall be done through alternate means of communication like telephone or an SMS.

1.13.2. Employees shall consider splitting their E-Mails for added security. (Parts of the information sent in separate e-Mails) as per business requirement.

1.13.3. Use of IRM/PGP tools or digital certificates shall be deployed.

1.14. Special Precautions to employees when sending External e-Mails:

1.14.1. Unless properly authorized, e-Mail must not be used to create legal or contractual obligations such as ordering goods or services. Under no circumstances must company credit card details be given by e-Mail. If it is necessary to purchase goods or services that are advertised as being available only by purchase using e-Mail, contact the Procurement Department. Where there are genuine business needs for e-Mail based contractual transactions, properly secured e-business solutions can be developed. Where contractual negotiations are taking place through e-Mail, ensure that a contract is not unwittingly entered into by, for example, using the phrase “subject to contract”.

1.14.2. Before sending an e-Mail which contains information of a commercial nature (e.g. price information of any kind, information that concerns another supplier, technical information), check it carefully (including attachments) to ensure that it has been addressed correctly, that it only contains information you would wish the addressee or potential forwarding addressees to see that it is factually correct. If in any doubt concerning the content of the e-Mail, contact the appropriate Commercial department for your business e.g. Supplies, Commercial, Sales.

1.14.3. Assume that the e-Mail shall be widely circulated within the receiver’s organization. Therefore, if you wish circulation to be restricted, specifically state so in the e-Mail, for example "not to be copied or forwarded to anyone without the specific consent of the sender". In the majority of cases that include information of a commercial nature you should include your management as a copy addressee.

1.15. E-mail Etiquette

1.15.1. Style

1.15.1.1. E-Mail carries no cues to help the receiver interpret the tone of the message other than the words used themselves. Attempts at humor or irony often fail to be picked up by the receiver, leading to misunderstandings and sometimes open hostility. It is wise to re-read messages written in the heat of the moment before sending them to ensure that they will not cause unintended offence. E-Mails can be used as evidence in legal proceedings.

1.15.2. Attachments

1.15.2.1. Wherever possible put the whole message within the body of the e-Mail rather than using attachments. This enables the search engines to find key words in the document, making retrieval and searching at a later date faster and easier. Where an attachment has to be used to preserve the document’s format, it is a good idea to put a brief description with some key words in the mail message that carries the attachment to enable the search to find it later.

1.16. Other Good Practices

1.16.1. Take care to ensure that mail addresses are entered correctly, especially if the mail is to be sent externally. Use the company Address Books to check the names of internal recipients.

1.16.2. Keep address lists short by sending e-Mails to only those who need them. Use "cc" for people who do not need to take action on your note.

1.16.3. Use BCC is not a good practice and shall be avoided.

1.16.4. Do not include the original attachment when replying to senders.

1.16.5. Do not send junk mail, house move announcements, invitations, advertisements etc.

1.16.6. Be careful on receipt of an e-Mail from an unrecognized source; it may contain a virus that could have a severe effect on the company network. If the source cannot be verified in another way, do not open any attachment but delete the e-Mail message.

1.16.7. The Internet cannot assure delivery of e-Mails. If a reply to your message is not received within the expected time the recipient may not have received your message.

1.16.8. If an e-Mail is received which is not meant for the user (i.e. wrongly sent), then, if possible, the user should inform the sender and also delete the mail.

1.16.9. Always use one mail for one subject.

1.16.10. Only mark CC to those where necessary.

1.16.11. Zip large attachments when sending them.

1.16.12. For communication with external parties use PDF.

1.16.13. Use of read receipt, delivery status shall be used with extreme discretion and care.

1.17. Disclaimer

1.17.1. Standard disclaimers shall be set on external e-Mail messages. IT shall ensure that automatic disclaimers are affixed to all outgoing mails. Corporate Communications Team and Legal team shall ensure that language and content are in line with business requirements and meet current business and legal requirements; respectively.

Responsibilities

The responsibilities lies with the following personnel:

- All Employees/users
  - To protect information assets and follow the e-Mail, Policy.
  - To report breaches or violations.
- For IT systems, IT/IS departments will
  - Establish and deploy security policies to support compliance with this e-Mail Policy and ISO 27001
  - Circulate tips and good practice of e-Mail to educate users
  - Implement appropriate logical access controls (e.g. within Active Directory)

  - Follow License Agreements for all deployed software.
  - Log access and help in conducting audits.

Enforcement:

- This policy and procedure is applicable for all the employees of the company who have access to and use the information assets and IT assets as listed in the Information Asset Classification sheet which have been created for all the departments. Any violation shall be dealt in accordance with the disciplinary action process as laid down in the Code of Conduct.

- Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the rights to alter or amend any clause in this document at any time as per its discretion.

Metrics

- The metrics shall be generated by the IT Security Team once every 30 days.

- The points include as given below, but not restricted to.
  - Number of requests for increase of mailbox size
  - Number of emails with no signatures
  - Number of emails exception approvals
  - Email Usage by employee
  - Mails sent to public mail sites.
  - Unauthorized applications on tablets and mobiles
  - Number of active accounts of employees who have been transferred / resigned/terminated.
  - Employees caught sending chain mails and inappropriate content.

Exceptions

- Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reasons existing at any point of time.

- Exceptions to this Security Policy and Procedures shall be allowed at the time of implementation of this policy and procedures or at the time of making any updating to this document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which shall be of temporary or permanent in nature.

- All exception requests shall be submitted by respective HODs/ Security In-charge. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.

The Security In-charge shall review all exceptions, as the case may be, every year for validity and continuity.

Disclaimer

- JMBGRP reserves all rights and is the exclusive owner of all intellectual property rights over this Acceptable usage Policy and Procedures document. This document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (such as electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior consent from the Apex Committee. The Acceptable usage policy and procedure document is meant to be published on the intranet of JMBGRP and/or any other forum as decided by the management of JMBGRP. Anything not specifically stated in this Acceptable usage policy and procedure document shall not be considered as implied in any manner.

- For any clarifications related to Email Security Policy. and procedure document with respect to its interpretation, applicability and implementation, please raise a request in Ticketing Tool.

References:

- Control: A.5.14