Information Security Management System
Acceptable use of information assets Policy

Document no. JMBGRP/ISMS/Pol-AU

Version no. v1.2

THIS DOCUMENT IS PRIVATE PROPERTY OF J. M. BAXI GROUP MUST NOT BE REPRODUCED, DISCLOSED TO ANY THIRD PARTY, OR USED FOR ANY OTHER PURPOSE WITHOUT PERMISSION IN WRITTEN FROM J. M. BAXI GROUP

Document details

Classification	Internal	
Released date	28.08.2018	
Description	This policy document describes the acceptable usage of information asset and what is not permitted when using the company's information assets.	
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 "12. Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "Scope, Policy, Procedure"	

Contents

Purpose

Information is one of the important assets of an organization for taking business decisions and maintaining competitive advantage. Information can be stored in many forms, such as data stored in computers, emails, videos, printed & hand-written material, verbal communication etc. Information assets (information and computer hardware, IT systems and networks) need protection for confidentiality, integrity and availability.

This policy describes what is permitted and what is not permitted when using the company's information assets.

Scope

This policy applies to all employees; (Business owners, custodians, system administrators, software developers and users of information.)

The policy also applies to other stakeholders such as outsourcing partners, customers, suppliers, consultants, trainees, external processing agencies and distributors whenever they are provided with access to the organization's information and assets.

Policy

- Employees have access to and will be entrusted with Secret/ confidential information assets related to trade secrets, finances, transactions, dealings, plans, strategies, affairs, research and development activities, products, services, technology platforms and processes amongst others as per the Information Security Policies and Procedures of JMBGRP.
- Employees are expected to abide by the laid down policy and procedures and thereby ensure the usage of and access to information assets is done in acceptable manner.
- This policy shall be applicable for JMBGRP employees during their tenure with the company and shall continue to remain in force post the cessation of employment as well.
- JMBGRP employees shall agree upon the clauses and conditions as laid down in the Code of Conduct and the appointment letter.
- Public information shall be handled in accordance with the guidelines as laid down by Corporate Communications.
- Usage of information assets and information systems shall be aligned to the business requirements only.
- While using the information assets and information systems at JMBGRP, employees shall ensure that laws of the land are not violated in manner.
- All incidents related to misuse of information assets and information systems shall be reported in a formal manner.
- While using the information assets and information systems, employees shall not trespass privacy of any of their fellow employees.
- JMBGRP reserves the right to question and audit employee action and apply disciplinary action should a violation be identified.

Procedure

1.1. The procedure covers the following points:

1.1.1. Communication to users.

1.1.2. During & After Employment.

1.1.3. Information Processing Facilities:

1.1.3.1. Computers (Desktops, Laptops, Smartphones, Tablets).

1.1.3.2. Personal Devices.

1.1.3.3. Facsimile (Fax).

1.1.3.4. Photocopier.

1.1.3.5. Network Printers.

1.1.3.6. Secure Deletion of Digital Data.

1.1.3.7. Secure Deletion of Paper Data.

1.1.3.8. Cupboards/Fire Proof Cabinets.

1.1.3.9. Networking Points.

1.1.4. E-mail.

1.1.5. Internet.

1.1.6. Information Handling.

1.1.7. Back-up of Data and Applications.

1.1.8. Information in Transit: Paper Assets.

1.1.9. Information in Transit: Digital Assets.

1.1.10. Employee Hygiene

1.1.11. RFID Hygiene

1.1.12. Visitor Etiquette

1.1.13. Monitoring of Usage: Mail, Internet.

1.1.14. Right to Scan, Check and Audit.

1.1.15. Incident Reporting.

1.1.16. Handy Cams/ Digital Cameras

1.1.17. Air Conditioning

1.1.18. UPS

1.1.19. Telephones

1.1.20. Laminating Devices

1.1.21. Binding Equipment

1.2. **Communication to Users**

1.2.1. Information assets need to be handled and protected in accordance with their classification as defined as Public, Internal, Confidential and Secret. The DO's & DONT's for protecting Info Assets should be communicated to the users in the following ways:-

1.2.1.1. Dedicated Portal for Incident

1.2.1.1.1. For employees to have access to Policies and Procedures, Training Content, Calendar to inform them about the activities conducted across various departments and locations.

1.2.1.1.2. To communicate events, circulars and action points from Security In-charge office.

1.2.1.1.3. To act as a repository of the Risk Assessment and Information Asset Listing documents / Articles related to security, Security Best Practices amongst others.

1.2.1.1.4. An incident reporting portal to lodge incidents related to Information Security.

1.2.1.2. Information Security Training, Testing and Evaluation shall be done for every employee of JMBGRP through the E-Learning Portal. It is mandatory for each employee to get a score of 75%, failure to do so will entail repeating the test until such time the employee gets the minimum score of 75%. Refresher Trainings shall be conducted by the HR of the department and through E-Learning Platform on best practices and end-use hygiene shall be followed.

1.2.1.3. Over and above the E-Learning Portal, it shall be the responsibility of every HoD to ensure that all employees in the department have understood in spirit and intent the rationale of Information security.

1.2.1.4. All employees shall provide a declaration stating compliance to the laid down policies and procedures. By taking a declaration from each employee that there shall be compliance to the information security policy and procedures.

1.2.1.5. HoD shall communicate the relevant aspects of the procedures to the third-party personnel working in their department and using information assets of JMBGRP.

1.3. **During and After Employment:**

1.3.1. Employees shall not share/modify/delete the business information, either during their employment (except in the proper performance of their duties) or at any time (without limit) after the cessation of employment, directly or indirectly:

1.3.1.1. Use for their own purposes or those of any other person, company, business entity or other organization whatsoever.

1.3.1.2. Disclose to any person, company, business entity or other organization whatsoever; any Critical or Confidential Information relating to or belonging to JMBGRP.

1.4. The restriction above will not apply to Information which:

1.4.1. Is already in the public domain other than by way of unauthorized disclosure or an employee is entitled to disclose under the Public Interest Disclosure; or an employee is required to disclose by law; or expressly authorized in writing by the MD to use or disclose.

1.5. The Company may at any time during the employment or on the termination of employment require employees/ vendors to return all documents (including all notes, original documents, extracts and summaries) and other information storing media relating to the business or affairs of the Company or any Group Company which are in their possession. These shall include all copies and reproductions.

1.6. Employees shall not at any time during employment make any copy, record, notes or memoranda (whether or not recorded in writing or on computer disk or tape) relating to any Confidential or Critical Information, other than in the performance of their duties pursuant to the terms and conditions of employment / engagement.

1.7. Employees shall read and sign the Confidentiality / Non-Disclosure Agreement and conformance of the same shall be taken on an annual basis by e-mail. Employees shall understand their duty and obligation to hold confidential, any information with regards to the identity of the companies by whom JMBGRP have been approached, are quoting to or transacting business.

1.8. **Information Processing Facilities:**

1.8.1. Information processing facilities are devices or utilities used to handle information; e.g. personal computers, laptops, printers, smart phones, tablets, mobiles, services applications amongst others. Information processing facilities are provided by the organisation to employees and other stakeholders for the organisation's business purpose only and they should use it responsibly.

1.8.2. Therefore employees shall not share or solicit to share, exchange, create, store distribute information either in digital or non-digital form which may cause slander and or attempt to slander, defame, disrespect individual employees, employee groups, religious or social values as professed by employees within JMBGRP, allude to or fuel development of acrimony and or discontent amongst employees and also violate the Indian Law in any manner.

1.8.3. This procedure there seeks to articulate the steps which shall be followed in spirit and intent by the employees of JMBGRP through in the usage of information assets and information processing facilities of JMBGRP in an acceptable manner so as to meet the company's objective of providing a secure business environment and also ensuring compliance with the applicable laws.

1.8.4. **Computers (Desktops, Laptops, Smartphones, Tablets)**

1.8.4.1. **Users shall:**

1.8.4.1.1. Make any procurement/ installation of hardware or software only after consulting the IT/ and approval of HoD.

1.8.4.1.2. Ensure that all assets like PC's, printers and other peripherals are tagged. If the asset tagging is missing, users should contact the IT Service Desk and inform them accordingly,

1.8.4.1.3. Switch-off their phones /Tablets in the Board Rooms/ VC Rooms/ TP Rooms / Meeting Rooms.

1.8.4.1.4. Disable the Blue Tooth / NFC of their Smartphones / Tablets.

1.8.4.1.5. Physically handle PC's and laptops with care.

1.8.4.1.6. Keep the working area free from any corrosive material, liquids and eatables.

1.8.4.1.7. Use only licensed software approved by the IT Team.

1.8.4.1.8. Use corporate anti-virus software and ensure that this is updated

1.8.4.1.9. Dispose-off the equipment according to company guidelines through Admin/Maintenance/IT Team as the case may be.

1.8.4.1.10. Secure laptops with a security cable if left unattended in open areas

1.8.4.1.11. Store laptops, in a locked drawer or cupboard when away from the office if it is not necessary for you to carry them.

1.8.4.1.12. Carry laptops/ Tablets only as hand baggage during air travel whenever possible

1.8.4.1.13. Register laptops at Site Security gates when going into/ out of company premises if required by local procedures

1.8.4.1.14. Observe manufacturer's instructions for protecting the equipment at all times, e.g. protection against exposure to strong electromagnetic fields.

1.8.4.1.15. When at home, users shall keep company Laptop/Blackberry/Smartphones/Tablets away from access to family members including children.

1.8.4.1.16. Shall protect the access through a PIN/Password as the case may be for mobile devices.

1.8.4.1.17. Not write PINs and Passwords on pin boards, stick pads or personal diaries.

1.8.4.1.18. Passwords shall be complex as stated in the Password Policy & Procedure.

1.8.4.1.19. Ensure that critical and confidential data is backed up through IT Team support on a centralized portal.

1.8.4.1.20. Only portable media as approved by IT Team shall be used.

1.8.4.1.21. Declare the possession of unauthorised media to HoD and IT Team and do the necessary migration to the company approved media.

1.8.4.1.22. Shall ensure through IT Team that the individual machines are patched and all the latest antivirus updates have been installed.

1.8.4.1.23. Always press "ctrl+ alt +del" and "enter" or press "windows +l" to lock the screen of your desktop or laptop.

1.8.4.1.24. Shall only be connected to conditioned power supplies.

1.8.4.1.25. Usage of remote access / connectivity tools, P2P tools, IP Messengers shall not be permitted on JMBGRP network.

1.8.4.2. **Users shall not:**

1.8.4.2.1. Exchange or share credentials to access systems and services.

1.8.4.2.2. Interchange or move assets without informing IT Service Desk and obtaining necessary approvals.

1.8.4.2.3. Add/ remove/ change any part of the asset without informing IT Service Desk and obtaining necessary approvals. The assets should be used as provided by the IT Team.

1.8.4.2.4. Install any unauthorised or offensive / in appropriate screen savers.

1.8.4.2.5. Make changes to the default configuration settings made by IT Team (IP address, proxy, anti-virus settings, host names, enabling or disabling of services any means) of any IT equipment without approval from the IT Team.

1.8.4.2.6. Try to gain access to desktops and laptops of other employees.

1.8.4.2.7. Take computers/ printers home without prior management approval which will be for a specific period, after which the equipment shall be returned.

1.8.4.2.8. Attach personally-owned laptops, Smartphones and Tablets or any such computable device capable of passing information in any form to the company's network.

1.8.4.2.9. View/ edit confidential information in public places where the screen can be seen by others.

1.8.4.2.10. Use personal internet connections using data cards, USB, Wi–Fi, Bluetooth devices, internet-enabled smart phones on organization owned assets (unless permission to do so).

1.8.4.2.11. Connect to the Internet while in office through a Data Card.

1.8.4.2.12. Allow anyone to use company laptops for non-business purposes including use by family members for gaming/ surfing the Internet, downloading and installation of content/ installation of software amongst others.

1.8.4.2.13. Initiate repairs / maintenance or modification to the devices provided.

1.8.4.2.14. Shall not access services, applications and information systems through public domain such as (airports, internet cafes and kiosks). There could be a possibility of key loggers being present.

1.8.4.2.15. Shall not download critical and confidential attachments on mobile devices.

1.8.4.2.16. Shall store personal information on company provided desktops/laptops/mobile devices. Compromise of personal information on company provided systems is not the responsibility of JMBGRP. However should there be legal consequence on account of such an act by the employee then JMBGRP shall initiate appropriate action against the employee.

1.8.4.2.17. Synchronization of smart phones with desktops/laptops shall not be allowed if not authorized.

1.8.5. **Personal Devices:**

1.8.5.1. It is prohibited to bring any personal information processing devices (Laptop PC, Smartphones and Tablets amongst others) onto company premises without management approval in writing stating reasons for the special requirement. Personal devices if allowed to be connected to the JMBGRP network shall the Network and Domain Policies of JMBGRP only.

1.8.6. **Facsimile (Fax) Usage:**

1.8.6.1. A record of all information assets which are faxed needs to be maintained in a Fax Usage Register.

1.8.6.2. It is recommended to avoid fax transmissions of CRITICAL and CONFIDENTIAL information assets.

1.8.6.3. Where required, the following procedure shall be practiced.

1.8.6.3.1. The owner shall fax the CRITICAL and CONFIDENTIAL information assets in person.

1.8.6.3.2. Request the recipient to be near the Fax machine and reconfirm the Fax number.

1.8.6.3.3. After confirming the recipient's presence near the Fax machine, start the transmission. At the end of the transmission, call the recipient and confirm the receipt.

1.8.6.4. Faxing of GENERAL Information assets shall be at information assets owners' discretion.

1.8.6.5. Fax machine shall not be used as regular telephone.

1.8.6.6. There shall not be individual fax machines provided to employees.

1.8.7. **Photocopying:**

1.8.7.1. Individual photocopier to be disallowed except for Security In-charge all the photocopiers shall be available on the company network with access control and ration paper to print across departments.

1.8.7.2. It is recommended to avoid photocopying of CRITICAL and CONFIDENTIAL information assets. However if required, the owner themselves shall be present while copying.

1.8.7.3. The owner shall sign upon the copy of CRITICAL Information Asset, assign copy in the form of "Page X of Y" numbers to all pages and handle as per Handling of Information Assets Procedure.

1.8.7.4. A record of all CRITICAL Information assets that are photocopied needs to be logged.

1.8.7.5. The photocopier used shall be password protected to prevent from any unauthorized access to photocopied material. This shall ensure that the creator of the CRITICAL information asset shall always be present when the process is going on.

1.8.7.6. Co-Located departments on the same floor shall have separate photocopier to prevent any unauthorized access.

1.8.7.7. The documents shall not be left behind unattended.

1.8.7.8. Malfunctioning of the equipment shall be reported to the maintenance team as an event.

1.8.7.9. Instruction manual and Dos & Don'ts shall be displayed for easy viewing.

1.8.7.10. Photocopying shall not be permitted outside JMBGRPs premise. If being done, the custodian of the asset shall be present during the entire process.

1.8.7.11. There shall be camera surveillance in photocopy areas.

1.8.8. **Network Printers:**

1.8.8.1. Individual printer to be disallowed except for Security In-charge all the printers shall be available on the company network with access control and ration paper to print across departments. If it is required as an exigency then prior approval from Security In-charge shall be sought in writing stating the reasons for the requirement.

1.8.8.2. It is recommended to avoid printing of CRITICAL and CONFIDENTIAL information. However, if required, the owner himself shall print it preferably on a local printer. In case of a network printer, the owner shall collect the printed documents immediately after giving the print command.

1.8.8.3. The owner shall sign upon the printed document and assign copy numbers to all pages, and handle it as per Handling of Classified Information Procedure.

1.8.8.4. The printing of GENERAL information assets may be carried out as per the owner's discretion.

1.8.8.5. The network printer shall be password protected.

1.8.8.6. Co-Located depts. on the same floor shall have separate network printers to prevent any unauthorized access.

1.8.8.7. The information assets shall not be left unattended at any given time.

1.8.8.8. Loss of assets shall be reported to HOD and logged as an event.

1.8.8.9. Malfunctioning of the equipment shall be reported to the identified IT Team as an event.

1.8.8.10. If printing is to be beyond office hours or on holidays then consent of the HOD shall be taken in writing.

1.8.8.11. Instruction manual and Dos & Don'ts shall be displayed for easy viewing.

1.8.8.12. Printing option shall be provided to authorize personnel as decided by HOD.

1.8.9. **Secure Deletion of Digital Data:**

1.8.9.1. Only as permitted by the HoD and through a written consent when the data in question has no business need.

1.8.9.2. Data shall be digitally shredded.

1.8.9.3. The concerned media shall then be formatted multiple times.

1.8.9.4. All deletion shall be done under personal supervision or with the support of the IT Team.

1.8.10. **Secure Deletion of Paper Data:**

1.8.10.1. All CRITICAL & CONFIDENTIAL Information Assets shall be shredded beyond physical reconstruction manually if no mechanical shredder is present.

1.8.10.2. If a mechanical shredder is present then the creator/owner shall shred the information asset personally and not assign the task to any other employee.

1.8.10.3. If the shredder is full then, it shall be emptied by the user or have the task done through housekeeping and then conduct the process of shredder.

1.8.10.4. Shredding of GENERAL and PUBLIC assets is left to the discretion of the asset owner.

1.8.10.5. The material to be shredded shall not be left unattended at any point in time.

1.8.10.6. The mechanical shredder shall also have the capacity to shred CDs/DVDs.

1.8.10.7. If mechanical shredder is not available then the CDs/DVDs shall be cut manually into min 4 parts or punched with a few holes using the paper punch.

1.8.10.8. Every department on the floor shall have its own shredder.

1.8.10.9. Malfunctioning of the equipment shall be reported to the identified IT Team as an event.

1.8.10.10. Bulk shredding if it is to be done beyond office hours or on holidays, then the consent of the HOD shall be obtained and shall be done in the presence of the concerned stakeholders only.

1.8.10.11. Instruction manual and Dos & Don'ts shall be displayed for easy viewing.

1.8.10.12. The shredders used shall have UL and ISI marking.

1.8.10.13. If location wise shredding is to be done by central admin at the end of the day and the activity shall be recorded. The area shall be kept under surveillance. The execution of the activity shall be under supervision of the Admin Person and a register shall be maintained to log the activity.

1.8.11. **Cupboards/Fire Proof Cabinets**

1.8.11.1. Critical Paper documents / media shall be stored in a fire proof safe with documented and restricted access. The index of the same shall be stuck inside of the cupboard storing the same.

1.8.11.2. All confidential assets shall be kept under lock and key in a segregated manner by way of a separate cupboard.

1.8.11.3. Clear desk (not keeping any paper on the desk, when not present at the work place) policy to be implemented. Confidential information should be locked away (ideally in a secure cabinet) when not required, especially when the office is vacated during travel, employees is not at the desk on account of meetings or at the end of the day.

1.8.11.4. Cabins, desks, cupboards and other storage spaces shall be locked at the end of the day. The keys shall be kept with an assigned person in the dept or copies of the keys shall be made available by the Administration team for department employees who need to access the Information assets.

1.8.11.5. The keys shall be available with HOD and only one additional person as assigned by the HOD.

1.8.11.6. The cup boards shall always be locked and this shall be checked at the end of the day before employees leave the office.

1.8.11.7. Non-functioning locks/lost keys shall be immediately reported to the Admin dept as an event.

1.8.11.8. For rearrangement of the contents or replacement of the cupboard is to be done beyond office hours or on holidays then the consent of the HOD shall be taken.

1.8.11.9. To prevent unauthorized physical access to storage area there shall be Biometric Access Control on the Record Room.

1.8.11.10. For GENERAL category of information, Head of department shall ensure that recovery strategies for paper documents are in place.

1.8.11.11. Q-code or barcodes shall be used on paper documents before storage to ensure speedy retrieval when required.

1.8.11.12. Suitable offsite storage shall be used for voluminous paper assets which are required to be stored on account of business or regulatory requirements, but do not have the requirement for conducting daily business activities.

1.8.11.13. Additionally the paper assets could be digitised and stored on a common portal with secure access mechanism. The digitised assets shall also have smart search capability.

1.8.12. **Networking Points**

1.8.12.1. Networking points shall be labelled by default. Only those shall be enabled where the identified user needs to be connected.

1.8.12.2. They shall be firmly ensconced on their boards.

1.8.12.3. The network cables shall be of adequate length.

1.8.12.4. The material used shall be fire retardant.

1.8.12.5. No hubs/switches shall be connected to the point(s) without prior permission from the identified IT team /HOD.

1.8.12.6. No wireless/ Bluetooth devices shall be connected to these network points without prior permission from the identified IT Team.

1.8.12.7. For sensitive and critical systems the network point shall have Mac ID binding.

1.8.12.8. Access log analysis on a periodic Basis through collection of logs on a centralized server with view rights only to log administrator.

1.8.12.9. Connection to wifi shall be stated in the Network Security Policy and Procedure.

1.8.12.10. Guests will be allowed to connect to the network through designated Guest Network Points only.

1.9. **E-mail: - Refer E Mail Policy & Procedure for details**

1.9.1. E-Mail accounts are provided by JMBGRP for official business purposes only. The users should follow the guidelines described in the E-mail Policies.

1.9.2. E Mail Log-In credential shall not be shared.

1.9.3. Public mail sites are prohibited for business use.

1.9.4. Forward mails to internal recipients or external recipients, “Reply All” without reason, BCC, Forward to
Public Mail Sites, Circulating Chain Mails; is prohibited.

1.10. **Internet: - Refer to Internet Policy and Procedure**

1.10.1. **Granting Access to the Internet:**

1.10.1.1. Access to the Internet will be provided to employees for business use after authorisation from the department Head. Once approved, the necessary access rights will be granted to the user for browsing and the same will be communicated to the user.

1.10.1.2. Internet access is given to specific users and these rights shall not be transferred or extended to others.

1.10.2. **Controlling Internet Access – Refer to Access Control Policy & Procedure.**

1.10.2.1. JMBGRP shall assign Security In-charge to monitor traffic of employee usage when on and off the company network.

1.10.2.2. Internet websites are categorised according to their content. To enforce safe browsing, various categories of web sites will be blocked at the company firewalls.

1.10.2.3. The categories to be blocked and allowed will be determined by Information Security Management after due consultation. The categories

which are blocked/unblocked by internet content filtering is defined and is approved by the MR. (A sample filtering policy is enclosed below).

1.10.2.4. Category 3 is allowed to all users.

1.10.2.5. Category 2 can be allowed if specific permission is obtained from the respective Chief justifying the need for such access for the user.

Blocked		Allowed
Category 1	Category 2	Category 3
Adult	Entertainment	Business
Crime	Job Search	Computing IT
Malicious	Investment Sites	Educational
Violence	Game	Search Sites
Government Blocking List	Matrimonial	E-mail Sites
Swimsuit Lingerie	Personal Belief, Culture	E-banking
SPAM	Clubs and Societies	News (without Video)
Gambling , Speculation	Chat	Health
Drugs and alcohol	Music & Video	
Dating	Discrete use of Social Networking sites beyond office hours	
Blogging Sites, Hosting Individual Blogs	AI tools and websites	
Underground sites (hackers, crackers amongst others)	Sports	
Tor network	Other companies email address	
Torrent Websites	Shopping	
	Travel- Tourism	
	Politics	
If any useful link is wrongly classified , please log via Ticketing Portal		

1.10.3. **Usage of the Internet:**

1.10.3.1. Internet access is provided for official business purposes. Occasional personal use outside working hours is permitted, but prolonged personal use is not allowed; such usage will be treated as violation and may result in disciplinary action.

1.10.3.2. No information relating to the organization may be posted onto the Internet without written permission from Senior Management. In case of doubt about material that may be posted Corporate Communications should be contacted. Note that information that is confidential, or any other information that may damage the reputation of the company, shall never be posted onto the Internet.

1.10.3.3. The Internet shall not be used to create legal or contractual obligations, such as ordering goods or services, unless it is part of normal business activities and has been authorized by Senior Management.

1.10.3.4. Material shall not be posted or downloaded that is obscene, malicious, threatening , hostile, abusive, vulgar, defamatory, profane, unethical or contains derogatory remarks relating to gender, race, religion, colour, national/ethnic origin, marital status, age, physical/mental disability, medical condition or sexual orientation, or anything else objectionable and not abiding by the law.

1.10.3.5. Official company information shall not be revealed in blogs, message boards, personal web sites etc.

1.10.3.6. Do not reveal official personal or organizational details to any website which is not relevant to company business (e.g. when completing forms to subscribe to newsletters) and do not use internal company passwords on Internet sites.

1.10.3.7. Internet postings are subject to the same legal rules that cover printed material, be it copyright protection, libel, criminal conduct, fraud etc. Internet postings shall therefore be proper, appropriate and factually correct.

1.10.3.8. Responsibility of Internet activities will rest with the user. The company does not accept liability for any personal damage or loss incurred as a result of Internet activity.

1.10.3.9. Any document being sent through the Internet goes into the public domain and therefore users should act accordingly regarding company confidentiality policies. If any confidential information has to be sent, it should be sent in an encrypted form by saving the document with a password. JMBGRP users may use an encrypted VPN tunnel - contact the administrator for queries.

1.10.3.10. Files for private use such as music, videos, photographs etc. shall not be downloaded.

1.10.3.11. Users should not download very large files during normal office hours.

1.10.3.12. Using the Internet for listening to the radio or any such activity which consumes bandwidth and does not have any business benefit shall not be permitted since such activity tends to congest communication pipe.

1.10.3.13. Social networking sites such as personal Facebook and any other social media amongst others shall not be used during office hours unless for legitimate business purposes. When used out of office hours or from home, it is prohibited to publish any official information relating to the company on any such public sites.

1.11. **Back-up of Data and Applications: - Refer Back Up, Restoration and Media Handling Policy & Procedure.**

1.11.1. For most of the IT systems, back-up process is ensured by the IT. However, employees are responsible for local data back-up which resides on user's PC's/ Laptops.

1.11.2. **Users shall:**

1.11.2.1. Identify the information residing on the PC's/ Laptops which needs to be backed-up. Users shall include all business-related files.

1.11.2.2. Ensure periodic back-up is done through a centralized tool which shall be provided by IT Team.

1.11.2.3. Contact the identified IT team if they need any assistance pertaining to back-up's.

1.11.2.4. Refresh the back-up at an appropriate frequency according to the level of change.

1.11.2.5. Test the recovery of the backup facilities at least annually.

1.11.2.6. Back-up data held on laptops at least weekly and before any off-site visits.

1.11.2.7. Data backed up on CDs and DVDs shall be encrypted or password protected. Gradually all data from optical media shall be transferred to a centralized back up platform as provided by IT Team.

1.11.3. **Users shall not:**

1.11.3.1. Take back-up copies/ data out of company premises without written permission from the HOD.

1.11.4. Appropriate disciplinary action may be taken in case of deliberate misuse of information assets.

1.12. **Information in Transit: Paper Assets**

1.12.1. To secure Critical & Confidential documents in transit within the same premises, there shall be document register for logging the dispatch of the document along with mail acknowledging the receipt from the receiver or shall be carried by the authorized personnel or shall be carried by owner whenever possible.

1.12.2. To secure Paper Critical & Confidential documents document in transit between two JMBGRPs locations, double Seal envelope with tamper proof taping and counter signature on all flaps and sign (full signature) across all openings and joints or specific courier shall be identified for Critical & Confidential documents items only or recipient shall send acknowledgement to sender via mail on receipt. Only company approved couriers shall be used.

1.13. **Information in Transit: Digital Assets**

1.13.1. All Critical digital information shall be compressed, encrypted and password protected before being mailed. Suitable IRM tools shall also be used to attach policies for access.

1.13.2. Information being shared through pen drives/ HDD then it shall be encrypted and password protected.

1.13.3. All Confidential Digital information shall be compressed and protected with a password.

1.13.4. An appropriate folder locking using user access control method shall be provided to restrict folder access.

1.13.5. Digital assets shall not be stored on any public cloud storage facilities e.g. Drop Box, One-Drive, etc., amongst others.

1.13.6. Information exchange by way of file transfers shall be done either through Secure File Transfer Norms, Or through shared folders with restricted access or through secure portals.

1.13.7. Use of Secure Communication Channel shall be deployed for Critical and Confidential when exchanging with external parties or internal employees.

1.14. **Employee Hygiene:**

1.14.1. All employees shall display their identification badge when on office premises.

1.14.2. All employees shall use biometrics coupled with RFID access control where ever deployed.

1.14.3. By default, all employees shall not be permitted entry to the identified secure areas like server rooms and data centers and other office areas as per the access control matrix and the zones created.

1.14.4. Tail gating is prohibited.

1.14.5. The list of banned items as displayed at security desk is applicable for employees/ external parties as well.

1.14.6. All employees will adhere to local security setup during entrance in the premises or at the gate.

1.14.7. Employee entry into office areas beyond office hours or reporting to work on holidays shall have the mail approval of the respective HOD and information provided to the building security.

1.14.8. If felt necessary employee bags may be checked at the entrance to ensure that banned items and or devices are not brought into the premises.

1.14.9. Carrying of critical and confidential paper assets out of office shall be done through prior approval of the HOD only.

1.14.10. Employees shall not discuss company matters in public spaces or in the presence of strangers.

1.14.11. Within the extended employees of JMBGRP, information shall be shared on a strict need to know basis.

1.14.12. White boards in departments shall be kept clean after use.

1.14.13. No information asset shall be left unattended in the department.

1.14.14. Conference Rooms / TP Rooms/ Board Rooms/ Meeting Rooms/ VC Rooms shall be locked when not in use.

1.14.15. Phones shall be put in silent mode when entering the meeting. It will be the responsibility of the convener of the meeting to ensure discipline.

1.14.16. Employees shall refrain from working beyond office hours and on holidays unless there is an exigency and prior consent of the HOD has been taken and the concerned security desk has been informed. While entering and exiting the employee shall enter the register at the security desk.

1.14.17. Required Code of Conduct, Non-Disclosure Agreement, Confidentiality Agreement as warranted by business situation and need has been signed by every employee. Compliance to this point is the responsibility of the respective HOD.

1.15. **RFID Hygiene**

1.15.1. RFID card is the property of JMBGRP and shall be accorded the right attention and care.

1.15.2. For any loss of the identity badge, the employee shall inform the HOD/ Admin and Security and the Gate pass section of the location immediately through an e-mail /phone. The Gate pass section shall acknowledge the receipt of this mail within 1 hour from receipt and block access rights of the card which has been reported to have been misplaced or lost shall be recorded in the Incident Risk Register with the Security.

1.15.3. When the employee leaves the organization, the access card shall be returned to HR by the HOD.

1.15.4. **RFID cards Do's and DON'T's:**

1.16.4.1. **DO's**

1.16.4.1.1. Always hang the card by the LANYARD provided with the card.

1.16.4.1.2. Always carry the card while entering into the JMBGRP gates.

1.16.4.1.3. Always touch the card on the Reader while entering inside the gate.

1.16.4.1.4. Check for the RED/GREEN light.

1.16.4.1.5. Enter only when GREEN light shows.

1.16.4.1.6. Co-operate with the security Persons.

1.16.4.1.7. Provide your finger validation when asked.

1.16.4.1.8. Enter only when GREEN LIGHT is on.

1.16.4.2. **DONT's**

1.16.4.2.1. Bend the card.

1.16.4.2.2. Give your card to someone else.

1.16.4.2.3. Try to enter by using some else's card.

1.16.4.2.4. Mutilate the card.

1.16.4.2.5. Enter while RED light is on.

1.16.4.2.6. Fight with the security persons.

1.16.4.2.7. Don't enter when RED light is on.

1.16. **Visitor Etiquette:**

1.16.1. Visitors shall only come with prior confirmed appointment.

1.16.2. Visitors shall be allowed on premises during working days and during business hours only.

1.16.3. Reception to confirm with employee before visitor is allowed to meet.

1.16.4. Visitors shall be attended to in the visitor meeting rooms located on the ground floor of each building or shall be escorted by the host to the concerned office and escorted back to the exit.

1.16.5. In the building visitors shall be provided with a badge as per the zoning applied.

1.16.6. Visitor shall declare all items which are being carried inside in the premises. Entry shall be made of the computing devices and phones being carried inside.

1.16.7. Visitors shall be checked for banned items. If necessary, the security guard may also frisk the visitor.

1.16.8. Visitor gate pass shall be signed by the employee and the same shall be returned to the security during the time of exit by the visitor in the specific building.

1.16.9. If a multiple visit have been planned by the visitor, then the host shall escort the visitor to the next meeting venue and so on and so forth.

1.16.10. Visitors shall not carry any JMBGRP Asset without written documentation and completion of all the necessary formalities by the host.

1.17. **Monitoring of Usage: Mail, Internet**

1.17.1. The company shall monitor Internet usage of users without notice or approval and or consent. Monitoring shall be performed in accordance with company policy and national laws. If there is evidence that a user is not adhering to the requirements set out in this policy, the company reserves the right to take disciplinary action.

1.17.2. The company reserves the right to block or allow certain sites without prior notice and may withdraw access to the Internet for individuals if deemed necessary.

1.17.3. The company may monitor mail usage and contents thereof should a certain business situation warrant such a measure.

1.17.4. The company may also block certain mail IDS from sending mails to JMBGRP Network and vice versa.

1.18. **Right to Scan, Check and Audit**

1.18.1. The organization holds the right to scan, conducts forensic checks, monitor usage of laptops, desktops through Data Leakage Monitoring Tools, check and audit any information/ asset handling activities of an employee, if the situation warrants such an action. Any such activities will be done in accordance with company policy and national laws.

1.19. **Incident Reporting:**

1.19.1. Any misuse of information or non-compliance to the policies if noticed should be immediately reported to the IT Service Desk. If the action is critical or confidential in nature, the employer should report it to the Chief/ Head of Department.

1.19.2. The incident reporting procedure is detailed in the Incident Management Policy of JMBGRP.

1.19.3. Physical Security Incident shall be reported to Security officer:

1.19.4. IT Security Incident shall be reported on mail to : Security Incharge

1.19.5. There shall be provision on the web site to report incidents as well.

1.20. **Handy Cams/Digital Cameras – If they are to be used. By default, use of cameras is not permitted.**

1.20.1. Photography, bringing photographic equipment without written consent on premises is prohibited in JMBGRP.

1.20.2. Mobile phones and Mobile Devices are provided with a camera which is standard feature. However, any employee or visitor attempting to use the feature shall face disciplinary action.

1.20.3. Company owned equipment shall always be in the custody of the HOD and shall be released to any user with prior written authorization only.

1.20.4. No material shall be left in the memory of the digital camera. Any users who find it to be so shall report it to the HOD and shall delete the same after the owner of the material has downloaded the same.

1.20.5. Video Tapes/CDs/DVDs of handy cams shall be in the custody of the respective owners with respect to Confidential & General Information Assets and for Critical information assets, the same shall be kept in fireproof cabinet under lock and key with appropriate care as recommended by the manufacturer.

1.20.6. Usage of tapes and DVDs shall be monitored through a register and consent shall be sought from the HOD for Critical information asset.

1.20.7. Erasure of tapes or data on rewritable DVDs/CDs shall be done after necessary approvals from HOD.

1.20.8. Malfunctioning of the equipment shall be reported to IT Team team as an event and standby shall be provided to the department within 24 hours or as per the urgency of the department.

1.20.9. Personal use of the equipment shall be punishable as per the Code of Conduct Policy.

1.20.10. The Dos and Don'ts shall be clearly displayed, and the users shall be available at all times for the users.

1.20.11. Original packaging shall be retained with IT Team helpdesk; in the event the equipment has to be sent out for repairs.

1.20.12. The equipment shall have CE, UL, and ISI marking.

1.21. **Air-conditioning:**

1.21.1. Condensation if detected shall be reported to the Maintenance / Administration Dept.

1.21.2. All information assets shall be protected from getting damaged due to condensation.

1.21.3. Air conditioners shall be switched off at the end of the day.

1.21.4. Adequate temperature and relative humidity shall be maintained (24DegC and 50%) at the workplace at all times. This shall be checked on a fortnightly basis by Health & Safety and corrective action shall be taken.

1.21.5. Malfunction shall be reported to the Maintenance / Engineering as an event.

1.21.6. All switches shall be firmly ensconced on their panels.

1.21.7. Sockets shall be tamper proof.

1.21.8. The supply of 240 Volts at 5 amps shall always be maintained. If any specialized equipment requires any special supply, then the same shall be arranged through the Maintenance/ Engineering Dept.

1.21.9. They shall be placed in a manner which shall not affect movement at the work desk.

1.21.10. The wiring shall be fire retardant and shall be properly ducted or not exposed to any

external environment. There shall not be any exposed joints.

1.21.11. The wiring shall have the necessary quality assurance marking eg ISI, UL amongst others.

1.21.12. The switches and sockets and switchboards shall have the required quality marking such as ISI, UL amongst others.

1.21.13. Junction boxes shall always be locked, and appropriate signage shall be displayed.

1.22. **UPS (Un-interrupted Power Supply):**

1.22.1. UPS shall always be of online variety with a minimum back-up of a minimum of 2 hours.

1.22.2. The batteries used shall be long life maintenance free dry batteries.

1.22.3. All UPS points shall be labelled.

1.22.4. Portable UPS shall be switched off when not in use.

1.22.5. Equipment to be connected to UPS shall be in accordance with the capacity of the UPS. Inductive load such as fans shall not be connected to UPS. Air conditioners, heaters shall not be UPS.

1.22.6. Only UPS shall be used and not inverters as they have inherent switching problems and shall pose problems to the equipment in the office.

1.22.7. If a centralized UPS is present, then it shall be sited in a separate room for the same which shall be locked at all times and shall be accessible to the identified IT Team personnel only.

1.22.8. For the centralized UPS for the building then there shall be correct estimation of load by the Engineering & Maintenance team before commissioning.

1.22.9. Back up for existing UPS. This shall be aligned to business corroborated Recovery Time Objective (RTO), Recovery Point Objective (RPO), Maximum Tolerable Period of Disruption (MTPoD) in a documented manner so that optimum responses can be ensured.

1.22.10. Equipment malfunction shall be reported to the identified IT Team as an event.

1.22.11. UPS wiring shall be fire retardant and shall have ISI, CE, UL and IEC approval as the case may be.

1.22.12. The UPS shall have the required quality certificates such as ISI, UL amongst others.

1.22.13. Dos and Don'ts shall be easily visible and user's manual shall be easily accessible.

1.22.14. Access to UPS area shall be restricted to authorized personnel only.

1.23. **Telephones**

1.23.1. Access to the EPABX room shall be restricted.

1.23.2. It is recommended that phone line sweeps be conducted once in 12 months to

detect the presence of listening devices and parallel telephone lines.

1.23.3. Provide at least one direct telephone line without any parallel connection to the Senior Management.

1.23.4. All devices registered under voice communication applications viz; EPABX, EPABX peripheral's or patch panels from origination to termination, shall be secured from physical, fire or environmental issues.

1.24. **Lamination Device**

1.24.1. Any Critical information asset which has to be laminated shall be done so in the presence of the owner/creator of the asset only with prior approval from the HOD.

1.24.2. For Confidential and General information asset shall be at the user's discretion.

1.24.3. Every document laminated shall be logged in the register.

1.24.4. For bulk laminations for Critical information assets beyond office hours or on holidays, it shall be done under the consent of HOD and the owner/creator or the nominee shall be present during the activity.

1.24.5. Usage of the equipment beyond office hours or on holidays shall be with the approval from the HOD.

1.24.6. The lamination film used shall be used per the manufacturer's recommendation.

1.24.7. Dos and Don'ts shall be easily visible and the users' manual shall be easily accessible.

1.24.8. Malfunction of the equipment shall be reported to IT Team helpdesk as an event.

1.24.9. The equipment shall have quality marking such as ISI, UL amongst others.

1.25. **Binding Equipment**

1.25.1. Binding of Critical information assets shall be done in the presence of the owner/creator of the information asset only.

1.25.2. Binding of Confidential and General Information Assets shall be at the discretion of the owner of these assets.

1.25.3. Every document which has been bound, an entry of the same shall be maintained in the register.

1.25.4. Volume binding to be done beyond office hours or on holidays for Critical information assets shall be with the consent of the HOD, but in such cases the owner/creator or the assigned nominee shall be present.

1.25.5. Equipment malfunction shall be reported to the identified IT Team as an event.

1.25.6. The equipment shall have quality marking such as ISI, UL amongst others.

Responsibilities

- All Employees/users:
  - To follow Information Security Policies and Procedures in spirit and intent.
  - To report breaches or violations on the portal.
  - All company equipment and infrastructure shall be handled with due care and attention as recommended by the manufacturer.
  - All the employees shall comply and cooperate with surprise checks and audits.
  - Employee shall enforce visitor etiquette.
- For IT systems, IT/IS departments shall:
  - Establish and deploy security policies to support compliance with this Acceptable Use Policy and Information Security Management Systems.
  - Implement appropriate logical access controls (e.g. within Active Directory).
  - Follow License Agreements for all deployed software.
  - Log access and help in conducting audits.
  - Internal audit shall be done by Internal Audit team once in six months of all the depts. at the location.

Enforcement:

- Any employee found to have violated this procedure shall be subjected to disciplinary action as per JMBGRP Code of Conduct Procedure.
- 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 procedure at any time as per its discretion.

Metrics

- Metrics shall be measured and reported once every quarter to GIS.
- Metrics shall be measured by the HODs and IT Team where applicable.
- Given below are metrics to be measured but not restricted to:
  - Unauthorized software detected on laptops and desktops.
  - Unauthorized accessories usage detected on laptops and desktops.
  - Malfunction of equipment by dept. and location.
  - Number of print jobs fired by dept.
  - Number of faxes by dept.
  - Number of photocopies by dept.
  - Files last accessed by date/ by size on laptops and desktops.

- No of systems not updated with OS Patches, AV Updates and Service Packs.
- No of complaints pending beyond TAT.
- Number of corrective actions and preventive actions not closed as a part of Internal or External Audits.
- Number of laptops/desktops found with content by way music, video and software's.
- No of scans done for Critical and Confidential Information Assets.
- No of CDs and DVDs written.
- No of media (USB, floppies, DVDs and CDs) destroyed containing Critical and Confidential Information assets.
- Data loss due to exhaustion of backup time on UPS standalone and portable units.
- No of failed logins on desktops and laptops.
- No of 3rd party access sessions to JMBGRPs network.
- Number of lost RFID Cards.
- Number of third party vendors working on location/ for the dept with expired contracts.
- No of network complaints on account of network congestion on account of misuse by employees.
- No of deviation requests per dept.
- No of times fax machine has been used for telephony.
- Number of incidents on account late - working by employees.
- Number of employees working late.
- Number of employees working on holidays
- Number of third party personnel working beyond office hours and on holidays

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 reason existing at any point of time.
- Exceptions to the Information Security Policy and Procedures may have to be allowed at the time of implementation of these policies and procedures or at the time of making any updating to this document or after implementation on an ad hoc basis based on business or a specific and a peculiar manifestation of circumstances which shall be of temporary or permanent in nature.
- All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception Form and sign-off on the same shall be maintained including ad-hoc requests.
- Identified IT team 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 this Acceptable usage policy and procedure document with respect to its interpretation, applicability and implementation, please raise a request in Ticketing Tool.

References:

- Controls: A.5.10, A.8.1, A.8.19