Information Security Management System
Equipment Safety & Security Policy & Procedure

Document no. JMBGRP/ISMS/Pol-EQ

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document to protect all it-team equipment to prevent loss, damage, or compromise the information assets and interruption to business activity.	
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 “References” a	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: “Procedure, Responsibilities”	

Contents

Purpose

JMBGRP recognizes the need to protect all it-team equipment to prevent loss, damage, or compromise the information assets and interruption to business activity.

The Equipment Security Procedure outlines the controls and responsibilities to ensure protection of all IT equipment used by JMBGRP (owned/leased/rented) to reduce the risk of unauthorized access to the data on it and adequately safeguard all the supporting utilities. The same has been carried out by having documented and regulated processes.

Scope

All Locations of J.M Baxi Group in India

All Employees of J.M Baxi Group

Policy Statement

- This policy addresses the aspects of equipment siting and protection of desktops, laptops and network infrastructure equipment's(servers, routers, switches, firewalls and appliances), Data Storage devices like pen drives, CDs, External Hard Disks, PDAs, phone instruments, printers, scanners, copiers; hereinafter called as IT-equipment.
- It also addresses protection and siting of security of the cabling infrastructure, lighting systems, air-conditioning, generators, UPS systems, power substations and fire prevention and detection systems if any; hereinafter called as non-IT equipment's or supporting utilities. Wherever the word "equipment" is used, it means IT and non-IT equipment and has a business value and impact, shall it be compromised in any manner.
- The policy addresses reduction of risks through addressing weaknesses in hardware acquisition, movement and usage of equipment within the premises and outside the premises, disposal of equipment, re-use and ensuring proper maintenance of equipment through either in-house department or an outsourced vendor.
- Adequate protective measures shall be adopted for designated secure and work areas for the equipment housed in these areas along with the supporting utilities. These protective measures shall be deployed by the Administration/ Security department for non-IT equipment and IT Team for IT equipment's.
- Procurement of equipment shall be as per business requirements only and the necessary management approval taken before commissioning a new project or a facility.
- Basic minimum standards of safety, as mentioned by the product vendor, shall always be adhered to.
- Business equipment shall always be safeguarded against natural and manmade disasters.
- The siting of the equipment shall ensure that routine and emergency maintenance of the equipment shall be possible to be carried out effectively.
- Movements of equipment shall be tracked.

- Decommissioning / disposal of IT and non-IT equipment's shall be done through an established formal process and measures shall be deployed to ensure that no advertent or inadvertent loss of data / violation of any regulatory compliance take place.

Procedure

1.1. The procedure shall address the areas as stated below:

1.2. Procurement of Equipment

1.3. Siting and Protection of Equipment's – Data Center/NOC/SOC (Network Security Locations)

1.4. Securing of Desktops / Laptops: Dos' and Don'ts

1.5. Cabling Security

1.6. Malfunctioning of Equipment

1.7. Securing of Desktops / Laptops: Dos' and Don'ts

1.8. Maintenance

1.9. Movement of Equipment

1.10. Procedure for Media Handling

1.11. Loss/ Theft - Common process for laptop/desktop

1.12. Disposal of e-waste

1.13. Procurement of Equipment

1.13.1. Division/Department shall put laptop/desktop requirements to IT fulfilling the eligibility criteria. IT shall centrally obtain necessary budget for providing laptop/desktops including software to be installed, connectivity etc. and arrange delivery of the same. No laptops/desktops shall be procured by Divisions/Departments by themselves.

1.13.2. Where current equipment does not meet the requirements, IT team shall work out and document the detailed requirement specifications along with performance parameters to meet the desired functionality.

1.13.3. The IT team shall ensure evaluation of various equipment providing the desired functionality. The evaluation shall be carried out based on the parameters, but not limited to:

1.13.3.1. Compatibility with existing infrastructure

1.13.3.2. Impact analysis on the existing infrastructure

1.13.3.3. Vendor specified performance against the identified parameters.

1.13.3.4. Support available from the vendor.

1.13.3.5. Vendor stability

1.13.3.6. Alternatives

1.13.3.7. Cost benefit analysis

1.14. The IT Team shall forward the report to IT Head Network Infrastructure and Head End User Computing as the case may be.

1.15. Equipment procured shall undergo an acceptance testing before installing it to the live network. The acceptance test shall include parameters like:

1.15.1. Performance of the equipment against the vendor specifications.

1.15.2. Performance against acceptable values.

1.15.3. Impact on the existing infrastructure.

1.15.4. After commissioning, the servers will undergo a 24-hour burn-in test before being moved to the production environment.

1.16. Siting and Protection of Equipment's – Data Center/NOC/SOC (Network Security Locations)

1.16.1. Entry to the JMBGRP shall be restricted to only the authorized people. Access list shall be prepared and shall be reviewed periodically. This access shall also define time and days of access wherever necessary. Any deviation shall be through written consent of the Head Networking Team with justification. Beyond office hours and on holidays, there will be written confirmation provided by the Head of Networking Team with call back from the Security Desk for verification Team.

1.16.2. JMBGRP shall have biometric access along with RFID cards for access. The entrance shall have CCTV surveillance and there will CCTV surveillance inside the locations as well.

1.16.3. The CCTV Surveillance recording shall be maintained for a minimum of three months or as mandated by business.

1.16.4. There shall also be register maintained for entering details of the visit and the identities of the people who have visited the JMBGRPs.

1.16.5. Any civil housekeeping activities shall be done under the supervision from the deputed IT personnel.

1.16.6. All network equipment's at DC sites (Network Distribution Sites) are under lock and key arrangement.

1.16.7. IT equipment's such as routers, switches, appliances, and servers shall be housed on racks which have been correctly sized.

1.16.8. Siting of racks or stand-alone systems shall be done in a manner which shall facilitate easy movement of personnel when required for inspection or maintenance.

1.16.9. Adequate placement distance and air conditioning shall be maintained to prevent buildup of thermal pockets as recommended by the manufacturer.

1.16.10. Temperature and relative humidity measurement as recommended by the manufacturer of the equipment shall be maintained.

1.16.11. Smoke detectors and fire extinguishers shall be placed and ensured operational in the datacenter. Testing shall be done once every week and report submitted to the Head Network Team on a monthly basis.

1.16.12. The flooring, paint and ceiling shall be made of certified fire retardant and anti- static material and shall have adequate insulation properties to help maintain desired temperature levels consistently.

1.16.13. The flooring shall be elevated and shall provide room for segregated conduits for power cables, network cables and air-conditioning ducts. The cavity in the flooring too shall be air-conditioned to ensure optimum temperature distribution by reduction in differential temperature gradient to acceptable levels.

1.16.14. IT Team shall be ensured that adequate lighting is available at all times.

1.16.15. Noise and vibration emanating from the air-conditioning systems shall be kept as per industry norms through strict adherence to the manufacturer's recommendations.

1.16.16. UPS, in fallback mechanism, shall be used to ensure uninterrupted power at all times.

1.16.17. Provision of Power Generator shall also be made and back up of the primary generator will be preferred.

1.16.18. Erection and commissioning for UPS shall be as per manufacturer's recommendation to maintain vibration and noise levels to optimum levels.

1.16.19. There shall also be a provision of a back- up air-conditioning plant units for all the JMBGRPs.

1.16.20. Preventive maintenance plan shall be present for all the infrastructure equipment with AMCs and SLAs. The same shall be the case for equipment of supporting utilities.

1.16.21. Energy audits shall be done periodically by the Administration Team and augmentation of supporting utilities shall be done as per findings.

1.16.22. The UPS, Air-conditioning plants and DG Sets shall only operate on 50% of their rated capacity to enable scaling up during crisis or emergency.

1.16.23. List of emergency contact numbers shall be placed at the most visible location.

1.16.24. In the Data Center – inert gas fire extinguishers shall be placed. In other locations CO2/nitrogen/argon fire extinguishers, which shall be placed at shoulder height.

1.16.25. Employees shall be trained in the handling of the fire extinguishers and crisis response. Drills shall be conducted at least 2 times in a year.

1.16.26. No inflammable /corrosive material shall be allowed on premises. Appropriate signages shall be placed.

1.16.27. Dust trapping doormats shall be used.

1.16.28. No eatables shall be allowed on premises.

1.16.29. Push to talk equipment shall be provided at the locations and managed through a central control room.

1.16.30. Rodent management shall be conducted once every week.

1.16.31. Self-glow signages shall be placed inside the locations and also outside the immediate vicinity.

1.16.32. The premises shall not be used as a storage room for used or decommissioned equipment's.

1.17. Securing of Desktops / Laptops: Dos' and Don'ts

1.17.1. No liquids and eatables in the vicinity.

1.17.2. No connection to unconditioned power supply.

1.17.3. Securing laptops with a anti -theft cable when working out of office.

1.17.4. Performing shut down process as recommended by the manufacturer.

1.17.5. Overheating shall be reported to the IT Helpdesk.

1.17.6. Exposure to heat shocks and dust shall be avoided.

1.17.7. Those working in Ports, project sites shall be provided with toughened laptops(based on management approval and as per business requirement)

1.17.8. Laptop shall not be left unattended in car; the user shall always ensure that the laptop is carried on person.

1.17.9. If the laptop/desktop has to be taken for offsite repair then the HDD shall be removed by IT and kept is safe custody.

1.17.10. For laptop /desktop which are being repaired on site, the end user shall be present during the activity.

1.18. Cabling Security

1.18.1. Power and communication lines are protected from interception and damage.

1.18.2. Power cabling is as per the standard laid by JMBGRP project department.

1.18.3. Communication Cabling for equipment's connection is guided by best caballing practices.

1.18.4. Cable diagrams for networks shall always be readily available with the IT Team and those of electrical supply and telecommunication systems with the Administration Team.

1.18.5. Cables shall be labeled distinctly to maximize identification and minimize handling errors.

1.18.6. Power, telecommunication and networking cables to information processing facilities shall be concealed via conduit to provide adequate protection from natural elements, rodents. All three categories shall be segregated to prevent cross talk and interference. Dress all Data cables on the left side of the rack and all power cables on the right side of the rack.

1.18.7. Avoid dressing cables tightly over sharp edges of railing or panels.

1.18.8. Ensure that cable connections are not stressed from any cable or chassis movement.

1.18.9. Bend radius for cables shall be as per product / vendor specifications. Special care shall be taken for fiber cables.

1.18.10. The electrical cabling in the work areas and secure areas shall be of fire-retardant material and insulated as per product norms.

1.19. Malfunctioning of Equipment

1.19.1. Malfunctioning of the equipment shall be treated as an information security incident (Refer to Incident Management Policy and Procedure)

1.20. Maintenance

1.20.1. Equipment maintenance is in accordance with the manufacturer's Instructions as per the process mentioned in the outsourcing contracts. The maintenance of utilities like power supplies, fire extinguishers are done through the procedure.

1.20.2. The maintenance of network equipment, desktops and laptops shall be done through SLA with the respective vendors whose risk assessment has been done and have been found to be suitable for the services required.

1.20.3. Critical and Network Equipment shall have the shortest TAT and this shall be documented based on the call history, frequency by the vendor and ratified by the IT Team

1.21. Movement of Equipment

1.21.1. The movement of equipment's, outside and return of equipment's, shall be recorded by the Asset Manager in the information asset inventory register.

1.21.2. Reconciliation shall done basis the inward and outward gate pass entries every month. Inconsistencies shall be recorded as an incident.

1.21.3. A suitable form shall be provided to initiate the movement of equipment. Alternatively, all equipment shall have Tracking system Tag which shall be recorded into a central application and upon receipt at the destination it shall be recorded there again by the concerned IT person.

1.22. Procedure for Media Handling

The quality of the compact disc is adversely affected by fingerprints, dirt, scratches, and due to decrease in the amount of light reflected from the recorded surface, CDs shall be handled with care as described below:

1.22.1.1. If the disc becomes soiled, gently wipe the surface with a clean, soft cloth, wiping from the center of the disc to the outer edge. (Do not use volatile chemicals such as benzene, thinners, record sprays or anti-static agents, which can damage the disc.) If a cleaner is needed, use a solution of mild neutral detergent.

1.22.1.2. Do not attempt to play cracked or warped disc. Shall a player exhibit playability problem, substitute another clean/new disc to determine whether the problem is in the disc or player.

1.22.1.3. Be sure never to touch the signal surface when handling disc. Pick up discs by grasping the outer edge, do not affix paper or tape to the disc, and avoid scratching the side of the disc which contains the label (contents of disc).

1.22.1.4. As with traditional audio vinyl records, compact discs are made of plastic. To avoid warping, keep the discs in their cases, and do not store them in direct sunlight.

1.22.2. **Preservation of Magnetic Tapes/Cartridges:**

1.22.2.1. Magnetic Tapes shall be labeled as per relevant procedure and kept in cool and dry place, free of magnetic field.

1.22.2.2. Magnetic tape shall be discarded after expiry of it-team shelf-life

1.22.2.3. Tapes shall be tested from time to time to prevent fungus formation.

1.22.2.4. These shall be placed in fireproof storage.

1.22.2.5. Cataloguing shall be done for the media and there shall be nominated person in IT who will manage media library.

1.22.3. **Protection of Media in Transit:**

1.22.3.1. Tapes, drives shall only be carried in a shock proof case. Anti-Static sleeves jackets shall be used for the primary packaging during movement. The case shall be locked and sealed.

1.22.3.2. Hard Disk and other magnetic media shall be packed using manufacturer's procedures for protection against environmental hazards, shock etc.

1.22.3.3. Package shall be addressed correctly to reach safe destination.

1.22.3.4. Either the media shall be carried by the nominated personnel from IT or the service provider.

1.22.3.5. Recipient shall acknowledge the receipt in writing to the sender.

1.23. Loss/ Theft - Common process for laptop/desktop

1.23.1. User shall file an formal complaint with relevant Govt. body.

1.23.2. Log a call in IT Helpdesk

1.23.3. Send copy of the FIR to IT Helpdesk

1.23.4. IT shall try to arrange working laptop/desktop/shared desktop, based on availability, for business continuity till permanent replacement happens as follows:

Specific to Laptop

1.23.5. In case of loss of a laptop, the user shall have to procure on his own the same model, configuration, specification of laptop/desktop that was stolen and have it included in the inventory and then use the same. In case same model is not available, equivalent model and configuration, specification (which is the standard at that time in the company) shall have to be purchased by the user. All expenses for procurement of new replacement laptop/desktop shall be borne by the user. Order documents (proof of purchase) for the same shall need to be submitted to IT for inclusion into the inventory
and subsequently allow it-team usage by the user.

1.23.6. IT shall arrange to get the company's asset records updated for this change. There shall be an increase in life of the asset as a result of such a purchase. In such cases, Instead of the user who has paid for the purchase of the new replacement laptop/desktop shall be allowed to buy that specific equipment at the end of four and half years (4.5 years) at nominal value.

Specific to Desktop

1.23.7. Department shall obtain budgetary approval to get new desktop until user is found responsible for the loss/theft in which case the cost shall be borne by the user. This shall be substantiated by the investigation report.

1.24. Disposal of e-waste

1.24.1. All scrapped IT equipment shall be disposed through Government Certified e-waste disposal vendors in an eco-friendly manner. This shall be done and coordinated by Head of the department of the company.

1.24.1.1. IT vendor who is responsible for hardware maintenance & support of servers, routers, switches, firewalls, appliances , desktops and laptops; shall coordinate the safe removal of data from this equipment prior to disposal. All configuration settings of firewalls, routers, and switches shall be reset to factory default. Digital shredders shall be used to securely delete data from decommissioned servers, laptops, and desktops. A written document shall be provided to the Head IT or the End User Computing Team, as applicable. Once all activities are completed, confirmation shall be provided to the Head of IT. E-waste disposal vendor(s) shall provide certificates for Disposal of e-waste in eco-friendly manner as per governmental norms

1.24.1.2. On exception, with MD's approval, scrapped IT assets may be donated to agencies under Corporate Social Responsibility (CSR) initiatives. The condition being the recipient has to agree to dispose such IT equipment after use in an eco-friendly manner.

Responsibilities

The responsibility for implementing this procedure lies with the following personnel:

- Departmental Implementer:
  - Asset Inventory is updated periodically.
  - Preventive and corrective action suggested.
  - Compliance to regulatory requirements.
- Engg. & Maintenance Team:
  - Capacity Planning, Procurement, Testing, Commissioning of equipment and performing Energy Audits and consequent augmentation of supporting utilities.

- Preventive and corrective maintenance activities.
- SLA and AMC review.
- Supervision and routine checks to ensure optimum uptime.
- Maintain records for outgoing and incoming equipment along with regular updates to the asset inventory system.
- Secure disposal/decommissioning of equipment.
- Compliance to regulatory requirements.
- Providing protection from natural and manmade disasters.
- Site inspection when starting new facilities.

- Network Infrastructure Team:
  - Capacity Planning, Procurement, Testing, Commissioning of equipment and consequent augmentation of Infrastructure requirements based on business needs.
  - Preventive and corrective maintenance activities through onsite and offsite support.
  - SLA and AMC review.
  - Supervision and routine checks and supervision to ensure optimum uptime.
  - Maintain records for outgoing and incoming equipment along with regular asset inventory updates.
  - Secure disposal/decommissioning of equipment.

- Physical Security Team:
  - Verify the outgoing Asset with the description in Gate Pass and Asset Transfer Form and verify the authorization.
  - Maintain gate-pass records for audit purposes.
  - Personnel access to secure and work areas.
  - Physical Access management to locations.
  - Recording Incidents and providing assistance in closure.

- Health & Safety Team:
  - Conduct Fire Equipment Testing and ensure that it is functional, adequate and current.
  - Conducting Fire Safety Audit.
  - Conduct Fire Safety and Evacuation Trainings
  - Conduct Drills

Enforcement:

- This policy and procedure is applicable for all the employees and contractors 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 with 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 it-team discretion.

Metrics

- The metrics shall be measured by the IT Team on a quarterly basis.
- Suggested metrics, but not restricted to.
    - No of breakdowns with SLA uptime data, corrective actions for exceptions.
    - Breakages in equipment transfer.
    - Equipment breakdown due to natural causes like rain/heat/condensation.
    - Number of times UPS/ DG/ Air-conditioning has not functioned when required during breakdown or contingency.
    - Number of times equipment has failed due to overheating.
    - Reconciliation of materials register for equipment which have left without gate passes and also entered without gate pass.
    - Number of equipment not traceable/lost/stolen on account of any records being maintained.
    - No. of equipment disposed off for which no record is maintained.
    - No. of Hard Disks/Tapes not being erased/ degaussed before being disposed of.
    - Number of laptop / desktop thefts in a month.
    - Equipment for which SLA have expired and not renewed.

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 the Personnel 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 could 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 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.5.4, A.5.16, A.5.17, A.5.18, A.6.1, A.6.2, A.6.3, A.7.1, A.7.2, A.7.3, A.7.5, A.7.6, A.7.7, A.7.8, A.7.9, A.7.10, A.7.11, A.7.1 A.7.12, A.7.13, A.7.14, A.8.1