Information Security Management System

Desktop, Mobile Computing & Teleworking Policy & Procedure

Document no. JMBGRP/ISMS/Pol-DM

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document to ensure desktops and mobile computing facilities provided to its employees and third parties to facilitate in their working and make communication with their fellow colleagues at JMBGRP or external premises efficient and productive.	
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 Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "Policy Statement, Procedure, Responsibilities"	

Contents

Purpose

JMBGRP has provided desktops and mobile computing facilities to its employees and third parties to facilitate their working and make communication with their fellow colleagues at JMBGRP or external premises efficient and productive. JMBGRP recognizes that the use of these facilities within and out of office premises poses various risks.

The Desktop, Mobile Computing & Teleworking Policy articulates the governing clauses which shall address the risks associated with physical protection, access controls, cryptographic controls, backups and mobile and malicious code protection in desktop computing, mobile computing and teleworking facilities.

Scope

All Locations of J.M Baxi Group in India

All Employees of J.M Baxi Group

Policy Statement

- This policy has been divided into 2 parts. The first part deals with the usage and expectations from employees and the second part deals with system security controls which are necessary for optimal and secure functioning.
- JMBGRP shall ensure that the desktops and laptops provided to the employees shall facilitate in discharging their professional duties as per planned outcomes. In order to achieve the said objective JMBGRP shall provide adequate and sufficient measures to be deployed either by of processes or through identified technology controls.
- To ensure mobile computing devices are maintained in a secure environment to minimize the threat of loss or theft of the device itself and any sensitive information it contains.
- A secure Access Control mechanism shall be provided when connecting to JMBGRP's network and shall have two factor authentication mechanisms implemented.
- An authorization process shall be established for provision of desktop, mobile computing and teleworking services, based on roles and responsibilities. Regular review and monitoring shall be done by the IT Team.
- Protection from malicious code, backup mechanisms and encryption shall be applicable on mobile phones, desktop, mobile computing and teleworking devices.
- Encryption controls shall be used wherever necessary as a means of data protection.
- Procurement of devices required for desktop computing, mobile computing and teleworking shall be through official channels only and shall abide by the security requirements of JMBGRP.
- At all times employees shall ensure that usage shall be aligned to business goals. Inappropriate usage shall be liable for disciplinary action. Users shall be responsible for the security of information held on such devices.

- Any change which the user wishes to be made on the system shall be affected only after relevant approvals from the HOD and the IT Team is received in view of the assessment of risk(s) if any.
- IT Team shall ensure that maintenance procedures of the systems shall be instituted and abided with.
- JMBGRP shall reserve the right to audit laptops and desktops on a random basis to ensure compliance to the company policy.
- Use of external data transmission and storage devices shall be as per the Acceptable Usage of Office Equipment Policy.
- System security controls shall be applied by IT Team and shall cover system maintenance, new program updates, patch management, antivirus management, protection from malicious code, system documentation and configuration management, use of system utilities and services, session time timeout.
- Network Security Controls shall be applied as per the Network Security Policy & Procedure.
- Necessary forensic tools / data leakage prevention tools / data leakage monitoring tools shall be deployed on laptops as per business need and circumstances.

Procedure

1.1. This procedure details the steps of employee responsibilities for usage of Desktops, Laptops and Teleworking.

Usage of Desktops and Laptops:

1.2. Issue Of Desktop/Laptops

1.2.1. Procurement of new desktops shall be as per the procured at rates as applicable for J.M Baxi Group and finalized by Procurement Team.

1.2.2. Desktops and Laptops purchased under various capital schemes shall also be as per JMBGRP's technical standard and approved make. No exception to this shall be allowed.

1.2.3. In case of a replacement, the department will take budget approval to get new desktop until user is found responsible for the loss/theft in which case the cost will be charged to the user as per the investigation report.

1.3. Acceptable Usage Norms Specific to Desktop

1.3.1. Employees using desktops shall ensure that :

1.3.1.1. The desktop provided is the property of JMBGRP and it shall be the responsibility of every employee to ensure that the asset is used efficiently and productively for business purposes only.

1.3.1.2. As the provided desktop is the property of JMBGRP, personal content shall not be stored on the machines.

1.3.1.3. Every desktop at JMBGRP shall be provided in a preconfigured Operating System (OS) Image. This OS Image shall have all the baseline configuration security settings as mandated by JMBGRP.

1.3.1.4. The Desktop shall have an asset identification number, in-case of damage to this number, IT Team shall be informed and the asset tag shall be restored.

1.3.1.5. Desktops shall be encrypted, with initial authentication occurring through the Encryption Tool Login, followed by a second level of authentication at the Active Directory (AD) login level.

1.3.1.6. The HDD on the Desktop shall be partitioned to have Operating Systems / Mails / Business Data. Through policy settings users shall not be permitted to store data on the partition containing mails, operating system files.

1.3.1.7. Folder level permissions shall be assigned, which shall be restricted to the actual user to prevent data leakage / theft on account of intentional or unintentional logical access.

1.3.1.8. IT Team shall be setting the Desktop Security Configuration Policies aligned to the security requirements of JMBGRP. Any attempt to violate those policies by attempting to make changes shall mandate disciplinary action.

1.3.1.9. Employees shall not install or attempt to install any free ware, shareware, tools, software, widgets, movies, songs, amongst others which does not have any approved and demonstrated business need and has also not been approved by IT Team. Presence of aforementioned material could create legal and regulatory issues for JMBGRP and also impact the reputation of JMBGRP.

1.3.1.10. Login Credentials used by employees shall not be shared under any circumstances. Doing so shall be considered to be serious incident and shall merit disciplinary action.

1.3.1.11. Employees shall not perform any concurrent Log In. If they encounter a situation, then the same shall be reported to IT Team in writing.

1.3.1.12. When they leave the desk, they shall lock their screen using “Ctrl + Alt + Del” and “Enter” or pressing ‘window key and L’ at all times.

1.3.1.13. When the employees leave for the day, the machine shall be switched off.

1.3.1.14. If any update process has been initiated by IT Team then the same shall not be aborted.

1.3.1.15. Connection of personal phones / mobile devices shall not be permitted as this will lead to the exposure of malware to the JMBGRP network. No phone

synchronization tools shall be installed, without prior consent and approval through HOD in writing.

1.3.1.16. Downloading of content from the internet shall only be permitted if there is an approved business need articulated and approved by the HOD. Exceptions such as these shall be for specific period and shall be revoked after the said period.

1.3.1.17. While in office data card shall not be connected to the desktop. Only JMBGRP network shall be used.

1.3.1.18. Centralized back up tool shall be provided by IT Team upon approval from HOD to the desktop users.

1.3.1.19. Data exchange via IP Messenger or any other Peer-to-Peer (P2P) tools is prohibited. Only approved communication tools, such as Google Hangouts, shall be used for data exchange.

1.3.1.20. Network shares shall be disabled by IT Team. Any such share which is still present shall be reported to IT Team and corrective action shall be initiated.

1.3.1.21. Employees shall also not attempt to open the desktop's Central Processing Unit (CPU), doing so will merit disciplinary action.

1.4. The following devices shall be referred to as Mobile Computing Devices for in the procedure document:

1.4.1. **Laptops**

1.5. The Mobile Computing and Teleworking procedure have been defined to address safety and security in Mobile Computing and Teleworking. This shall include physical protection, access controls, encryption controls, backups and protection from malicious and mobile code

1.6. Issue of Mobile computing devices (Laptops).

1.6.1. Laptops shall be provided in a phased manner, as and when their existing desktop computers become due for refresh and replacement.

1.6.2. Laptops for officers at all other locations shall have to be approved by respective HODs. Such approvals shall clearly state the need and risk such as :

1.6.2.1. Job involves extensive traveling, and the officer needs to be in touch with office/IT system,

1.6.2.2. Job involves working from more than one location,

1.6.2.3. Job involves providing online support by the officer to his/her function from outside office,

1.6.3. Technical standard, configuration, make & model of laptops shall be decided by IT Team. Support and services for these laptops shall be available in the company through maintenance contracts finalized by IT Team. Laptops shall be procured at rates which are applicable for J.M Baxi Group and finalized by Chief, Procurement. Laptops purchased under various capital schemes shall also be as per J.M Baxi Group technical standards and approved make. No exceptions to this shall be allowed.

1.6.4. Laptops have to be connected to J.M Baxi Group Active Directory and must have approved software as standardized by IT Team installed. Users are NOT authorized to load any other software which are not approved by IT Team.

1.6.5. During the term of usage, requests for any change of hardware or software must be routed through IT Team. Such requests should be recorded in IT Helpdesk. Users shall not install any hardware or software on their own.

1.6.6. Laptop users shall not be provided with "Administrator Access" to their machines.

1.6.7. All user laptops shall have endpoint encryption tool installed. Authentication shall be done at the encryption level to have access to the working environment and the second level of authentication shall be that of the AD (Encryption Tool is installed based on business requirement).

1.6.8. Employees shall not install or attempt to install any freeware, shareware, tools, software(s), widgets, movies, songs, amongst others which does not have any approved and demonstrated business need and has also not been approved by IT Team. Presence of aforementioned material could create legal and regulatory issues for JMBGRP and also impact the reputation of JMBGRP.

1.6.9. IT Team shall also install a content filtering on all laptops, to prevent misuse when not on the network.

1.6.10. IT Team shall provide a centralized back up mechanism for all laptop users.

1.6.11. Each and every laptop shall have the asset tag as per the company's procedure and in case of damage to this asset tag, the concerned user shall initiate remedial action through IT Team.

1.6.12. When travelling users shall refrain from connecting to Wi-Fi hotspots as these shall provide unauthorized access to external parties / intrusion of malware/spyware.

1.6.13. Users shall secure the laptop with a secure lock when on offsite locations.

1.6.14. When travelling the laptop shall not be left unattended and shall always be with the user.

1.6.15. Whitelisting of media shall be done and only company approved portable media shall be used. All such USB drives and portable hard disks (HDD) shall be encrypted prior to their handover to the employee by IT Team.

1.6.16. When travelling for long duration / overseas, IT Team shall ensure that a complete image back up is taken of the user machine, to ensure availability of the user data during emergencies and or compromise.

1.6.17. IT Team shall ensure that all unnecessary services on the mobile computing devices shall be disabled. Audits shall be carried out once a quarter as instructed by Information IT Team or when user reports a problem. Examples of such services include Bluetooth and Infrared amongst others.

1.6.18. Use of Bluetooth shall not be permissible on JMBGRP laptops.

1.6.19. While in the office, users shall not use data card or configure a hot spot on their phones through which they use the internet.

1.6.20. Anti-Virus Software / OS Patches shall be updated on laptops on a periodic basis. This shall entail that users shall connect with the network at least once in a month to get a refresh of new policies/patches/updates.

1.6.21. The HDD on the laptop shall be partitioned to have Operating Systems / Mails / Business Data. Through policy settings users shall not be permitted to store data on the partition containing mails, operating system files.

1.6.22. Folder level permissions shall be assigned, which shall be restricted to the actual user to prevent data leakage / theft on account of intentional or unintentional logical access.

1.6.23. IT Team shall always install a standard reference image of the Operating System, hardened to meet the baseline security configuration as per the organizations, when required to do so.

1.6.24. Exchange of data over IP Messenger or any such P2P tools shall not be permitted.

1.6.25. Network shares shall be disabled by IT Team. Any such share which is still present shall be reported to IT Team and corrective action shall be initiated.

1.6.26. Employees shall also not attempt to open the laptops on their own accord , doing so will merit disciplinary action.

1.7. Third Party / Vendor Laptops/Desktops on JMBGRP's network

1.7.1. **Refer to Third Party Security Policy for details.**

1.7.2. Briefly stated all third party / vendor machines which need to connect to the JMBGRP network shall abide by JMBGRP's domain policies.

1.7.3. The machines shall be liable to be audited.

1.7.4. The audit logs shall be enabled.

1.7.5. If required, the machines could be subjected to forensic investigation.

1.7.6. If required, JMBGRP shall also deploy, DLM (Data Leakage Monitoring) or a DLP (Data Leakage Prevention) solution on vendor machines.

1.8. Teleworking – Working from Home/ Offsite Working – In coordination with HOD and IT Team

1.8.1. The form for remote access available on Intranet for Dialup connectivity is used for application of such access. User shall raise the request through Ticketing Management tool and apply through departmental head to IT Team.

1.8.2. The user shall submit a request for teleworking to the concerned HOD reporting manager. The request shall also contain the time period for which access is required.

1.8.3. IT Team shall provide the teleworking facility to the employee and also explain the controls which are applicable and the responsibilities of the employee towards safe and secure use. This shall be done through a log on prompt which make the user accept the terms of use. Once the user accepts, this acceptance shall be stored against the username. Revocation of teleworking facility shall be done as per Logical Access Security Policy and Procedure.

1.8.4. The access provided shall be logged in the centralized database and shall be managed by the concerned team.

1.8.5. The IT Team shall ensure the review of central database periodically by Network / System Administrator to check for expired access. Expired access shall be blocked and disabled a per change request form.

1.8.6. VPN ACL (Access Control List) shall be reviewed on a quarterly basis, for usage time, applications worked on, mail sizes, by profile.

1.8.7. Session logs shall be maintained for every user who uses remote access

1.8.8. Laptops shall have a whole disk encryption (As per business requirement).

1.8.9. During teleworking and otherwise, the user shall not copy data from the office machine to any personal machine or portable media.

1.8.10. Personal laptops shall not be permitted to be used for official work.

1.8.11. Exceptions shall be reported as a part of MIS by the IT Team.

1.8.12. Company employees must normally use company-owned and configured equipment to connect to the company networks. Use of other equipment, such as the employee's home PC, is generally not allowed. Out-of-hours IT support staff should be provided

with company laptops for the purposes of remote support.

1.8.13. All software that is used for business purposes on the PC must be properly licensed.

1.8.14. Refer to Network Security Policy Document – IT Team

1.9. In case of Loss/Theft

1.9.1. User shall file complaint with Govt. body.

1.9.2. Log a call in IT Helpdesk

1.9.3. Send copy of the FIR to IT Helpdesk

1.9.4. IT Team shall try to arrange a working laptop based on availability, for business continuity till permanent replacement happens as follows:

1.9.4.1. 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 assessed 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 Team for assetisation. IT Team shall get the laptop assessed and allow its usage by the user

1.9.4.2. IT Team 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, the officer who has paid for the purchase of the new replacement laptop/desktop shall be allowed to buy that specific equipment at nominal value.

1.9.4.3. Laptops shall be insured.

1.10. In case of damage/repair : Desktops/Laptops – In coordination with IT Team

1.10.1. User shall be responsible for maintaining their machines in good physical condition.

1.10.2. If the desktop/laptop or any of its component(s) is physically damaged, the cost of repair will be charged back to the department. In case the user is held responsible for the damage, the cost will be charged to the user.

1.10.3. Users shall not attempt to or open the desktops CPUs /laptops to initiate or attempt any repair/maintenance procedure.

1.10.4. Users shall not attempt to remove any of the internal fixtures/panels.

1.10.5. The user shall not initiate any repair steps independently but will hand over the machine to IT Team for further action.

1.10.6. Laptop users also shall not independently go to the vendor or service center and have

their machine serviced/repaired.

1.10.7. For all onsite repairs the user shall ensure that the repair is done in their presence.

1.10.8. For any offsite repairs, it shall be the user's responsibility to back up Critical and Confidential Information through the assistance of IT Team on portable media and delete it from the HDD. Alternately it shall be a good practice to remove the hard disk before handing over the laptop for offsite repair.

1.10.9. For any repair/maintenance related activity, a call shall be logged on to the IT Team helpdesk.

1.10.10. Assurance report shall be prepared by the Head – End User Computing Group and provided to the Head Tech Support and Network Architecture on a monthly basis.

1.11. Return of Asset In case of transfer, retirement, resignation: Desktops / Laptops – In Coordination with IT Team

1.11.1. In case of transfer within the company, Laptop user can carry the laptop to his/her new place of work. All Desktop users will return the asset to earlier department in working condition. The returned machines shall be in the same configuration as they were provided earlier to the employee.

1.11.2. Such changes in place of work or return of asset shall be logged in the IT Helpdesk to record the change in asset database.

1.11.3. In case of transfer to any other JMBGRP Group company in India or overseas, Desktop Users/Laptop Users shall not be allowed to carry their desktops and these shall be surrendered to their department in working condition. The returning of the asset is to be logged with IT Helpdesk.

1.11.4. In case of resignation or retirement, employees would have to return their desktop to earlier department. Clearance & Settlement of dues would be done after the laptop with all accessories or desktop, as the case maybe, is returned in working condition. In case, after retirement the person is engaged as consultant, the person will be able to retain the asset after due approval from respective HODs.

1.11.5. IT Team shall assist the HOD to take the necessary back up of data of the employee in transition.

1.11.6. IT Team shall assist the HOD in providing with the backup of the laptops of the employees who are transiting.

1.11.7. In case the laptop is returned in non-working condition or incorrect configuration, the cost of repair shall be recovered from the user.

1.11.8. Assurance report shall be prepared by the IT Team – End User Computing Group and provided to the Head IT on a quarterly basis.

1.12. Refresh & Disposal of old laptops – In coordination with IT Team

1.12.1. A laptop shall be considered for refresh based on maintainability and technology, software compatibility etc. which may happen after completing four and half years of

use in the company. IT Team shall take necessary action for refresh.

1.12.2. New laptop shall be given by IT Team only on physically returning the old asset. The data on the old asset shall be preserved by IT Team for a period of one week for access by the user. Thereafter, clearance shall be taken from user and all data shall be deleted permanently from the hard-disk as preparation for disposal. Service provider, who was maintaining the asset, shall provide the users necessary technical & operational assistance in data removal. Data shall be digitally shredded on machines which are undergoing refresh and thereafter the HDD shall be formatted at multiple time.

1.12.3. Sale of old laptop to employee is not permissible (except the case where it has been purchased by an employee when original laptop was lost / stolen).

1.12.4. Old laptops which are owned by the company, after replacement, shall be disposed as per e-waste disposal guidelines issued by By-Products Sales. IT Team shall ensure that all the data has been formatted beyond reconstruction through digital shredding.

1.12.5. Assurance report shall be prepared by the IT Team – End User Computing Group and provided to the Head IT on a monthly basis.

1.13. Other devices: For Laptops/Desktops

1.13.1. All USB drives and USB hard-disks issued to users shall be registered with IT Team and shall be assigned an asset number for tracking. Random audit shall be conducted by the IT Team on USB drives and USB hard-drives for data carried by them.

1.13.2. Loss of USB drives and USB hard-drive shall be treated as an incident and shall be handled as per Incident Management Policy and Procedure.

1.13.3. All USB HDD and pen drives shall be encrypted using company approved tools.

1.13.4. Pen drives shall not be used as regular data storage devices.

1.13.5. Employees shall not connect any Switch Hubs, Blue Tooth Dongle, Wi-Fi antennas' to their machines.

1.13.6. Employees also shall not connect DVD writer's recorders/ printers / scanners / copiers / fax machines if not authorized to do so to their desktops/laptops

1.13.7. Portable storage shall be subject to random audits by IT Team.

System Security Control:

1.14. User creation

1.14.1. User registration and deregistration is carried out in controlled manner:

1.14.1.1. The users send in their requests for registration to the Ticketing Tool through the respective departmental heads.

1.14.1.2. The requests are sent for approval to Corp IT head and to the IT team for SAP user registrations.

1.14.1.3. The respective operations teams do these user registrations.

1.14.2. User Registration is done as per the procedures listed below by Outsourcing partner. For list of vendor procedures through the Ticketing Tool.

1.14.3. De-registration to the information systems is carried out using the respective procedure.

1.14.4. Ticketing Tool shall be used for the process of user creation. Going further an integrated Identity and Access Management shall be deployed to automate the process of user creation and deletion across all systems and applications.

1.14.5. Going further an integrated Identity and Access Management shall be deployed which shall ensure better management and governance of end user access activity and violations, requests.

1.15. Connection to Local Area Network

1.15.1. The following procedure shall be followed before laptops, desktops, smart phones, tablets belonging to JMBGRP are connected to LAN:

1.15.1.1. Check to see if the device is registered for use in the JMBGRP network.

1.15.1.2. Check for latest Antivirus definitions.

1.15.1.3. Check and ensure that only licensed software is installed on the machines

1.15.1.4. In case of machines with critical data, the hard drive shall be encrypted (Based on Business Requirement).

1.15.1.5. IT Team shall assign the IP Addresses for the machines.

1.15.1.6. IT Team shall ensure that the system is hardened as per the baseline security standard at JMBGRP.

1.16. Connecting to Wireless Network

1.16.1. The requestor shall fill in the Access Request form and submit the form to the Head of the Department (HOD) (Based on Business Requirement).

1.16.2. The Head of the Department (HOD) shall forward the form to IT Team for approval.

1.16.3. After the approval has been received, the network team shall grant the required access by issuing a joiner ID.

1.16.4. IT Team shall assist the user to connect to the wireless network with the joiner ID.

1.16.5. A certificate for authentication shall be installed on the user system for future authentication requirements.

1.16.6. The user shall use his domain credentials to connect to the wireless network points in JMBGRP.

1.16.7. The Wi-Fi user group at JMBGRP shall not have administrative user access.

1.17. Clear Desk and Clear Screen Policy

1.17.1. Information and information processing facilities are protected from disclosure to, modification of, or theft by unauthorized persons, and controls are in place to minimize loss or damage.

1.17.2. This is done by the implementation of a "clear desk and clear screen policy "

1.18. Terminal Timeout

1.18.1. The System Administrator/ IT helpdesk shall configure inactive terminals for all systems to be 'timed out' after specific time frame of inactivity to prevent unauthorized access. For all desktops and laptops, it shall be 10 minutes. For all applications it shall be 5 minutes.

1.18.2. Approved screen savers with passwords shall be used to protect user systems.

1.18.3. Users shall lock their terminals and activate screen savers with passwords when the terminal is not in use to protect against information theft or modification of data.

1.18.4. For critical systems there shall also be limitation on connection time enforced which shall prevent unauthorized usage beyond office hours or before regular office hours. Critical systems shall be identified by the HODs.

1.19. Security of System Documentation and Configuration files – Through IT Team

1.19.1. System documentation shall include system configuration files, installation and decommissioning records, records of modifications, modifications done to applications and systems, application documentation.

1.19.2. As per the valuation cited above for the various categories of systems, the protection shall be in keeping with the classification done as per the Information Asset Classification.

1.19.3. All system documentation shall be managed by the IT Team. System documentation shall be available through Notes Database / Portal on a need to know basis.

1.19.4. Any changes to the system documentation shall be captured through the Change Management Process.

1.19.5. Any exceptions or deviations shall be through Exceptions and Deviations content delivery person as mentioned in the framework.

1.19.6. Access rights to the machine where system documentation is stored shall be provided to authorize personnel from IT Team.

1.19.7. Only designated System Administrators shall have edit privileges if necessary other users shall only have read privileges.

1.19.8. Scheduled backup of system documentation data and configuration files shall be done and tested as well, with a log of the activity being maintained.

1.19.9. Access to system documentation shall be through formal approval obtained from Head IT Team only.

1.19.10. All system documentation and configuration files shall be in an encrypted format.

1.19.11. All system documentation shall be stored on a dedicated system with two factor access control. Backup of this system shall be taken once every week.

1.19.12. System State Backups of critical systems shall be taken once every week and stored on the dedicated machine.

1.19.13. The repository of system documentation shall be an integral part of the Digital Rights Management.

1.20. Review of changes done to system documentation and system configuration shall be conducted by the person/team having expertise in various device(s) appointed by the Information Head IT with a periodicity of 90 days.

1.21. Maintenance of Systems – Through IT Team

1.21.1. The IT Team shall ensure that the backup of the data is taken before any system maintenance activity for desktops/laptops. (Refer to Backup, Restoration and Media Handling Procedure).

1.21.2. In case of critical assets, maintenance activities shall preferably be performed in the presence of the asset owner or his/her authorized representative.

1.21.3. Emergency repair disks shall be maintained for system restoration. Mirror image of the approved standard system configuration shall be used for faster and error free installations.

1.21.4. The System Administrator shall design the file system keeping the following points in mind:

1.21.4.1. Operating system program files, live application program files, device files or hidden directories with program files in them shall not be present in a user's home directory. These shall be installed in a separate file system or partition users have no access to it.

1.21.4.2. Test / Demo applications shall be installed and tested on a separate server. Live data shall not be given for testing and test data shall be sanitized.

1.21.4.3. A disk quota shall be assigned to the file system for each user, where the user's home directories are kept.

1.21.4.4. Any malfunction of the system shall be logged as incident.

1.21.4.5. Emergency change - Any change deviating from security hardening due to be done in emergency (having impact on the security hardening document) which cannot follow the change request procedure shall be approved by Head IT by mail and or Ticketing Tool.

1.21.5. Assurance report shall be prepared by the IT Team – End User Computing Group and Provided to the Head IT and Network Architecture on a Quarterly basis.

1.22. New Applications, Programs or Updates

1.22.1. The users shall not be allowed to download any new application or programs without an approval from the Head End User Computing Group, preceded by HOD justification and approval.

1.22.2. If there is a need of a new application or program, the user shall submit the request to his Department Head and process shall be followed as per Software Copyright Compliance Procedure.

1.22.3. The Antivirus Administrator shall install the required application or program in the test environment; scan it for viruses and send his approval if the application is free of viruses. Intimate the IT Helpdesk to install the application on user machine.

1.22.4. For any user exception approval of the HOD is required.

1.23. Use of systems utilities and other utility software – Through IT TEAM

1.23.1. The access to systems utilities shall be restricted as per the Access Control Policy and Procedure. In particular, users shall not be given access to the systems utilities.

1.23.2. Right for installation of software on the systems shall be restricted to System Administrators/IT helpdesk. The same shall be tested by system admin to check if any existing system applications or services or performance is getting affected.

1.23.3. All end user requests shall be approved by HOD and IT TEAM post risk analysis of the same.

1.24. Hardening of Systems

1.24.1. The Security In-charge shall be responsible for preparing of the Baseline Hardening Checklists for desktops and laptops. The IT Team shall deploy these checklists.

1.24.2. The IT Team shall ensure that only required necessary applications and services are installed as per the hardening checklist. The actual hardening of the systems shall be carried out either by the IT Helpdesk personnel or through a dedicated team within the IT Team.

1.24.3. The IT Team shall identify the patches required to be applied. The deployment of these patches shall be done through the IT Helpdesk using the JMBIT Assist platform.

1.24.4. Only necessary network protocols, services and ports shall be enabled, which are required by the applications and operating system(s) being used.

1.24.5. Access to system files on desktops/laptops shall be restricted as per Logical Access Control Policy and Procedure. The same shall hold true smart phones, PDAs and Blackberry phones as well.

1.24.6. Access to system and application files shall be blocked for all users through the hardening activity conducted. Essentially for this aspect to be effective all drives shall be partitioned into a minimum of two partitions e.g., C and D in which C drive shall have OS and other related applications and D drive shall have data.

1.24.7. Unwanted shares shall be removed. File and directory sharing shall be restricted to authorized personnel by applying appropriate file and directory access permissions.

1.24.8. The IT Team shall prepare a report confirming, conformations to the Hardening Check list and record exceptions (with reasons). Exceptions if any shall be escalated and necessary approvals sought from the concerned HOD and Information Security Team Head as per business requirement.

1.24.9. The Security In-charge shall periodically conduct audit of hardening activity and submit its report to the IT Team for them to prepare a Corrective and Preventive Action Plan which shall be executed with 90% compliance. This activity shall be done either through a tool or manually on a quarterly basis or when a new system is inducted into the network.

1.24.10. A tool shall be applied to manage configuration settings for windows and non-windows systems and those which are not on the domain. This tool shall also have remediation capabilities to ensure corrective action is taken without manual intervention.

1.24.11. Assurance report shall be prepared by the Head – End User Computing Group and Provided to the Head Tech Support and Network Architecture on a monthly basis.

1.25. Security from malicious code

1.25.1. System is protected from Spy-wares, Mal-wares, Mobile codes, destructive Cookies, Active-X controls by using the following controls

1.25.1.1. Software installation is controlled to desktops/laptops which are enforced using active directory.

1.25.1.2. Personal firewall is enabled in each laptops and desktops

Responsibilities

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

- IT Team
  - Ensure issue of laptop computing devices on approval of the concerned HODs or designated authority in the respective departments.
  - Ensure updating of Asset Inventory.
  - Ensure that all laptops have disk level encryption.
  - Approve Revocation for resignations/terminations/transfers after retrieval of a mobile computing device.
  - Reissue the device on approval of HODs.
  - Ensure the review of central database periodically by Network /

System Administrator to check for expired access of teleworking.

- Disabling expired access of teleworking.
- Inform the Infrastructure Team immediately in case of resignation, termination and transfer.
- Ensure that the laptop device is formatted before it is issued to another user.
- Ensure that a complete decrypted backup of the device is taken in case of resignation, termination and transfer.
- Ensure that security controls stated in the procedure are implemented on all the mobile computing devices.
- Check the devices and accessories on return of Circulation device.
- Ensure that a complete decrypted backup of the device is taken on retrieval of the device.
- Ensure that mobile computing devices are updated with latest anti-virus signatures and encryption software is installed.
- Ensure that all unnecessary services on the mobile computing devices shall be disabled and switched off outside the office premises or when not necessary.
  E.g.
  Bluetooth, Infra-Red
- Perform laptop audit through a tool to detect unauthorized downloads, check for patch and antivirus updates, license status of various tools/softwares and Operating System installed. Check to see if the configuration settings meet the JMBGRP baseline security configuration mapping.
- Audit registered portable media physically devices to check the contents or upon business need.
- Assign VPN Access, Monitoring of VPN access.
- Maintaining of SLA with vendor
- Erasure of data beyond retrieval during decommissioning or hand over to another employee.

- Department Head
  - Approve issue of laptops devices through a formal process in writing.
  - Review and approve the request for teleworking.
  - Make request to block network access including VPN, Internet when not required or when the periodicity for which it has been assigned has expired

- User
  - Users shall be responsible for the security of information held on their laptops.
  - In event of a loss of a mobile computing device, shall inform the Department Head, file a FIR with Police and give a copy to Infrastructure Team.
  - Take special care to ensure that business information is not compromised while using mobile computing devices.

  - Follow steps as stated for repair and maintenance.
  - Follow acceptable usage as articulated in this procedure.
  - Report incident to IT Helpdesk if any, promptly.

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 its discretion.

Metrics

- The metrics shall be measured by the Infrastructure Team. The periodicity of measurement shall be once every 60 days. These are but not restricted to as under
    - Number of unpatched, un- updated user machines vs inventory.
    - Number of unrevoked remote access vs authorized list.
    - Number of machines with unauthorized content on user machines.
    - Rejected remote access request.
    - Software compliance.
    - Number of unresolved incidents / security violations.
    - Number of thefts of laptops and desktops
    - Number of theft cases resolved.

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 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 with in Ticketing Tool.

References:

- Controls: A.5.10, A.5.16, A.5.17, A.5.18, A.7.8