Information Security Management System
End Point Security Policy & Procedure

Document no. JMBGRP/ISMS/Pol-EP

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	The policy document has been formulated to ensure that any unauthorized access to computing systems shall be prevented and the desired security posture shall be established, maintained and sustained.	
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”	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: 3,4,5,6,7,8,9	

Contents

1. Purpose 4
2. Scope 4
3. Policy Statement 4
4. Procedure 5
5. Responsibilities 13
6. Enforcement 14
7. Metrics 15
8. Exceptions 16
9. Disclaimer 16
10. References 16

1. Purpose

1.1. JMBGRP recognizes that its IT Infrastructure is exposed to security risks because of end user computing systems and related software vulnerabilities. The End Point System Security Policy has been formulated to ensure that any unauthorized access to computing systems shall be prevented and the desired security posture shall be established, maintained, and sustained.

2. Scope

This policy applies to the following:

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

3. Policy Statement

3.1. Formal security maintenance processes shall be implemented for ensuring adequate security at the end user computing system level. Access to end point computing systems shall be restricted to those people who need the information to perform their business functions on a strictly need to know basis. System documentation shall be protected against unauthorized access. The reference to the word "system(s)" hereafter in this document shall be construed as end point computing systems like desktops, laptops, smart phones, tablets. Wherever required to be stated separately, the same shall be done to elicit a particular detail. However, the security management of smartphones, tablets and blackberry devices has been articulated in the BYOD (Bring Your Own Device) Policy.

3.2. IT Team shall be responsible for ensuring that systems are updated and functional with current operating system patches and antivirus updates. The systems shall be hardened and appropriate maintenance activity shall be carried out for the system(s) to work optimally.

3.3. Use of system utilities which may override system or application control shall be done only under authorization.

3.4. Each user shall be provided a unique user ID and password. Password management shall be done to ensure that quality and complexity of passwords is maintained. A

formal user registration and de-registration process shall be established. The password complexity shall be as stated in the Password Policy and Procedure.

3.5. For critical systems, session time out and connection time out shall be enforced wherever possible. If required login procedures for these systems shall be secure and shall comprise of multifactor factor authentication techniques.

3.6. Systems shall be configured such that users shall be able to lock their terminals either manually or automatically to prevent unauthorized access.

3.7. Any changes done to the systems shall be through a formal change management process.

3.8. When any changes are done to the operating systems, then the new system shall be tested before deployment by the assigned personnel from the IT Team.

3.9. Suitable tool shall be deployed for managing integrated roll out of OS Patches and AV Updates and initiate remediation measures to remove inconsistencies in deployment.

4. Procedure

The procedure has been structured to address various aspects of end point computing system security and the corresponding measures / roles which need to be considered for creating a secure access environment. The areas covered in this procedure include.

4.1. Clear Desk Clear Screen Policy

4.2. Induction of New Systems

4.3. New Applications, Programs or Updates

4.4. Hardening of Systems

4.5. Access control

4.6. User creation

4.7. Connection to Local Area Network

4.8. Connecting to Wireless Network

4.9. Clear Desk and Clear Screen Policy

4.10. Terminal Timeout

4.11. Security from malicious code

4.12. Security of System Documentation and Configuration files

4.13. Maintenance of Systems

4.14. Data Protection

4.15. Patch Management

4.16. Use of systems utilities and other utility software

4.17. Anti-Virus - Handling a virus infection for Desktop/ Laptop

4.18. User DO's and DON'Ts

4.2. Induction of New Systems

4.2.1. Induction of new systems shall be done as per the procedure defined in Network Security Policy.

4.3. New Applications, Programs or Updates

4.3.1. 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.

4.3.2. 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.

4.3.3. 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.

4.4. Hardening of Systems

4.4.1. The Information Security Team shall be responsible for preparing of the Hardening Checklists for desktops, laptops, smart phones, tablets. The IT Team shall deploy these checklists.

4.4.2. 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.

4.4.3. The IT Team shall identify the patches required to be applied. The deployment of these patches shall be done through the IT Helpdesk.

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

4.4.5. 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.

4.4.6. 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.

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

4.4.8. The IT Team shall prepare a report confirming, conformations to the Hardening Checklist 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.

4.4.9. The IT Team 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.

4.4.10. 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.

4.5. Access control

4.5.1. Refer to Access Control Policy & Procedure

4.6. User creation

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

4.6.1.1. The users send in their requests for registration to the systems through the respective departmental heads.

4.6.1.2. The requests are sent for approval to Head Security Team Through the Ticketing Tool for user registrations.

4.6.1.3. The respective operations teams do these user registrations.

4.6.2. User Registration is done as per the procedures listed by Outsourcing partner.

4.6.3. De-registration to the information systems is carried out using the defined procedures. IT clearance form shall be used.

4.6.4. Ticketing Management System 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.

4.7. Connection to Local Area Network

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

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

4.7.1.2. Check for latest Antivirus definitions

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

4.7.1.4. In case of machines with critical data, the hard drive shall be Encrypted (As per Business Requirement).

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

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

4.8. Connecting to Wireless Network

4.8.1. The requestor shall fill in the Access Request form and submit the form in the ticketing tool.

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

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

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

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

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

4.8.7. The WIFI user group at JMBGRP shall not have administrative user access.

4.9. Clear Desk and Clear Screen Policy

4.9.1. 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.

4.9.2. This is done by the implementation of a "ISMS/GDl-CDS/001: clear desk and clear

screen policy "

4.10. Terminal Timeout

4.10.1. 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 60seconds. For all applications it shall be 5minutes.

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

4.10.3. 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.

4.10.4. 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.

4.10.5. Critical systems shall be identified by the Programmed Managers/HODs and connection time and session time out shall be enforced wherever possible

4.11. Security from malicious code

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

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

4.11.1.2. Personal firewall is enabled in each laptop and desktops

4.11.1.3. Uncontrolled Internet access is not allowed; the content filter mechanism catches hold of Spyware, Malware etc.

4.11.1.4. Antivirus software is having Spyware and Malware control inbuilt.

4.11.1.5. Internet Explorer Security setting for Internet zones are high with at least

4.11.1.6. "prompt" any unknown code download.

4.12. Security of System Documentation and Configuration files

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

4.12.2. 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 Policy.

4.12.3. 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.

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

4.12.5. Any exceptions or deviations shall be through Exceptions and Deviations form as mentioned in the framework.

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

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

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

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

4.12.10. All system documentation and configuration files shall be in an Secured manner (Encrypted / Password Protected).

4.12.11. 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.

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

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

4.12.14. 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 IT Head with a periodicity of 90 (Ninety) days.

4.13. Maintenance of Systems

4.13.1. The IT 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).

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

4.13.3. 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.

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

4.13.4.1. 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.

4.13.4.2. Live or production data shall be kept in a separate file system with proper access control.

4.13.4.3. 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.

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

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

4.13.4.6. 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 department head by mail and or through the CRF (Change Request Form).

4.14. Data Protection

4.14.1. Disk level encryption can be used to ensure that the entire hard disk data is protected from unauthorized access. Refer to Encryption Procedure for details.

4.14.2. Use of USB ports, CDs/DVDs shall be restricted permitted in case of business need and after approval from HOD and/or Information Security Team through the exception form.

4.14.3. The name (NETBIOS) of the system shall not be indicative of the identity of the user of the system or the purpose for which the system is used wherever possible.

4.15. Patch Management

4.15.1. The IT Team shall ensure that current OS patches are identified, tested before they are deployed.

4.15.2. The relevant patches shall be installed on the systems remotely wherever required. Verification of this activity shall be done through a quarterly audit conducted by the Information Security Team and findings submitted to the IT Team for necessary implementation.

4.15.3. Patch updates on user machines shall be done either when the system is logged onto or when user decides to shut down or during the non-load hours of the day.

4.15.4. A tool- b a s e d approach shall be deployed to ensure that patch

management inconsistencies are ascertained and remediated without manual intervention.

4.16. Use of systems utilities and other utility software

4.16.1. 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.

4.16.2. 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.

4.17. Anti-Virus - Handling a virus infection for Desktop/ Laptop

4.17.1. Users shall promptly report any virus infections on their desktops / laptops to the IT Helpdesk. Refer to Incident Management Policy and Procedure should the following symptoms appear.

4.17.2. Program load and execution time taking longer than usual.

4.17.3. Alien graphics or messages appearing on the screen.

4.17.4. Excessive disk activity or processing time.

4.17.5. System unexpectedly “hanging” or “rebooting.”

4.17.6. Frequent and unusual error messages.

4.17.7. Unexpected disappearance of programs or files.

4.17.8. Executable files changing size for no obvious reasons.

4.17.9. The virus scanner informs that there is a virus

4.17.10. If a user notices a probable sign of infection on machine following actions shall be taken

4.17.10.1. The user shall disconnect the network cable

4.17.10.2. The user shall call the helpdesk for assistance.

4.17.10.3. The user shall not reboot the system until the help desk person arrives.

4.17.10.4. The user shall stop all processing and make a note of the symptoms and any messages that appear on the screen. If it is suspected that the message was initiated by opening an attached E-mail, a note shall be made of who sent the E-mail.

4.17.10.5. The help desk engineer shall check for viruses or other malicious code on the user's computer. It shall be ensured that the latest updates are applied for anti-virus programs.

4.17.10.6. In case of any infections, a backup shall be taken of the user's data and Anti-virus Administrator shall be updated about the infection for him to update the signatures.

4.17.10.7. If required, the helpdesk engineer shall use virus or worm cleaning tool for cleaning.

4.17.10.8. Procedures for cleaning of infections provided by the anti-virus software vendor must be followed.

4.17.10.9. In case the virus cannot be controlled internally, the IT-Helpdesk shall inform the IT Team. The external assistance, if required, shall be taken after the approval of the Head IT in consultation with the Information Security Team

4.18. User DO's and DON'Ts

4.18.1. The viruses and malicious code can propagate through different means including emails, usb drives, pen drives, CDS/DVDs, unauthorized software, downloaded content. The end users have a key role to play in guarding their machines / data against a virus infection

4.18.1.1. Users shall follow these guidelines to the utmost extent possible

4.18.1.2. Shall not attempt to change the scanner setting of their computers.

4.18.1.3. Shall ensure that virus definitions of the Antivirus scanner are regularly updated on their machines.

4.18.1.4. Shall ensure that personal firewall is enabled on their desktop / laptop if connecting to other external or public networks.

4.18.1.5. Shall always run the anti-virus software scans before connecting the portable devices to the network.

4.18.1.6. Shall not use floppies or CDs from unreliable sources.

4.18.1.7. Shall not install and use illegitimate software.

4.18.1.8. Shall not accept free software or use software given free with computer magazines, unless this has been approved.

4.18.1.9. Shall not browse or download content from unreliable sites on the Internet. These are typically underground and illegal sites.

4.18.1.10. Shall always scan the attachments for viruses before downloading them

5. Responsibilities

The responsibility for the planned initiative in this document lies with the following personnel:

5.2. IT:

5.2.1. Harden Systems (desktops, laptops, smart phones, tablets and blackberry phones.).

5.2.2. Keep track of software patches and apply appropriate patches on systems.

5.2.3. Enable appropriate access control settings.

5.2.4. Ensure that system maintenance activity is carried out under their supervision.

5.2.5. Categorize calls in terms of severe impact, moderate impact and medium impact and report on a monthly basis.

5.2.6. Call resolutions as per TAT (Turn Around Time) defined in the Incident Management Policy and Procedure.

5.2.7. Ensure the hardware and software meets the specifications before system induction.

5.2.8. Label system components and update asset inventory.

5.2.9. Create users as per Access Control policy.

5.2.10. Install software for protection against malicious code.

5.2.11. Ensure that system administration activities are logged.

5.3. IT-Helpdesk

5.3.1. Log Virus incidents.

5.3.2. Report incidents to Antivirus Administrator.

5.3.3. Guide users for corrective measures.

5.3.4. Install Antivirus software on all systems.

5.3.5. Update Antivirus signatures and updates.

5.3.6. Install approved applications only.

5.4. Users

5.4.1. Ensure that their systems have latest patches and are updated through an assurance note from the IT Team.

5.4.2. Ensure that their systems have antivirus installed and IT signature updated through the icon on the desktop.

5.4.3. Ensure that their systems have been hardened by permitting this activity to be completed on their systems by the Infra Team member.

5.4.4. Ensure that system maintenance activity is carried out under their supervision, if their systems have Critical and Confidential data.

5.4.5. Lock their terminals (Devices) when the terminal is not in use.

5.4.6. Log incidents through the IT Helpdesk

5.4.7. Users are expected to report any suspicious activity on their machines to IT-Helpdesk and adhere to this procedure.

5.4.8. Not download any new application or programs without an approval.

5.4.9. Follow the do's and don'ts mentioned in this procedure

5.4.10. Remove unapproved applications.

6. Enforcement

6.2. This policy and procedure are 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 Criteria sheet which has been created for all the departments. Any violation shall be dealt in accordance with the disciplinary action process as laid down in the Code of Conduct.

6.3. Violations by the vendors shall also come under the purview of the Information Security Framework and action shall be taken accordingly.

6.4. 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 asper IT discretion.

7. Metrics

7.1 The metrics shall be generated by the IT Security Team and reported to Security In-charge/ IT Head on a quarterly basis.

7.2 The metrics shall be measured; but not restricted to, are provided below.

7.2.1 Number of machines not hardened or hardened with exceptions.

7.2.2 List of patches not applied on the servers and desktops with reasons.

7.2.3 No of systems on whom maintenance has not been done and failures reported.

7.2.4 No of systems from where unauthorized software has been removed.

7.2.5 Number of system audits done for desktops, laptops, smart phones, tablets and phones.

7.2.6 Number of systems which have malfunctioned on account inadequate maintenance.

8. Exceptions

8.1 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.

8.2 Exceptions to this Policy and Procedures shall have to 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.

8.3 Any exceptions during implementation shall be submitted by the HODs responsible for the particular vendor. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.

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

9. Disclaimer

9.1 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.

9.2 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.

10. References:

Control A.5.13, A.7.8, A.7.11, A.7.12, A.7.13, A.7.7, A.8.1