Information Security Management System
Network Security Policy

Document no. JMBGRP/ISMS/Pol-NS

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document is to establish management direction, principles, and requirements to ensure the appropriate protection of JMBGRP's information on IT-Team servers and networks is 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 "13. Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "4, 8, 9"	

Contents

1. Purpose

1.1. JMBGRP has deployed an information technology infrastructure to facilitate IT-Team business and make it more efficient. Since the set of vulnerabilities & threats exist for any hosted service and established network, information security controls should be established and implemented which provide adequate protection.

1.2. JMBGRP shall provide a secure environment to all employees by adopting adequate and secure network and systems environment aligned with the business objectives.

1.3. The purpose of this policy is to establish management direction, principles, and requirements to ensure the appropriate protection of JMBGRP's information on IT-Team servers and networks is established, maintained and sustained.

2. Scope

2.1. The scope of this policy is applicable to all network equipment's, LAN, WAN links within the perimeter of JMBGRP network.

3. Policy Statement

3.1. The Network Security Policy shall apply to servers, routers, firewalls, IDS, IPS and other security appliances.

3.2. Formal security maintenance process shall be implemented for ensuring adequate security at the operating system level. Access to the operating system 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.

3.3. Use of utilities which may override existing 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. Before the deployment of the proposed change the same shall be tested on a test environment.

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. Changes done to the network devices comprising of siting or configuration settings shall be done through the existing process of change control by the concerned group at JMBGRP.

3.10. Employees and/or third parties using the network services of JMBGRP shall be provided with access rights on a need to know basis through a formal process.

3.11. Formal mechanism for recording and redressal of faults, events, incidents and problems shall be deployed by the IT Team.

3.12. Security controls like: management of system documentation, access control to identify network devices, services and applications, establishment of service level agreements with third party service providers for all outsourced services, equipment siting and protection, incident management and change control shall be implemented.

3.13. The Network Infrastructure of JMBGRP shall be managed and controlled so as to prevent internal and external threats to IT-Team information systems, applications, services which it offers. Adequate protection shall be provided for the same by of conducting Vulnerability Assessments and Penetration Testing (VAPT) along with Configuration and Access Rule Reviews. VAPT shall be conducted to ensure regular and periodic vulnerability assessment and penetration testing.

3.14. An integrated tool based approach shall be deployed which shall facilitate in the OS Patch Management, AV updating, inventory management, whitelisting of devices, whitelisting of applications, configuration management, monitoring of rogue network devices, license monitoring and compliance, usage of ports, power management; coupled with facility to initiate remedial measures.

3.15. Network shall be adequately protected from any possible threats emanating from Mobile Computing, Teleworking, Remote Access and internal traffic between users on the premises to prevent incomplete transactions, misrouting, unauthorized message alteration, duplication, abetment of fraudulent activity

3.16. Physical and logical access to diagnostic and configuration ports shall be restricted.

3.17. Segregation of network shall be done either physically between various business entities of JMBGRP or V-LAN architecture shall be established. In either case, Testing, Production and Development environment shall be segregated as well.

3.18. The roles and responsibilities coupled with segregation of duties for management of network security shall be clearly defined, communicated and reviewed on a regular basis to ensure optimum operative effectiveness and necessary segregation of duties shall be done to attain the said objective.

3.19. JMBGRP IT shall have documented SLA with vendors so as to provide uptime as mandated by business.

3.20. Monitoring of the identified network parameters shall be done by the Network Team to ensure optimal network uptime and user experience.

3.21. Secure log management process shall be established wherein logs getting generated at user, administrator level are captured. System-related log information shall be captured for further analysis and necessary action.

3.22. For the logged information to be consistent and meaningful, all the servers and networking devices shall have their system clocks synchronized either manually by the system administrator or an automated process using an AD server as reference.

3.23. If found necessary end user laptops and desktops shall also be monitored and employees shall comply with the same. Forensic investigations shall be done on the network components if warranted and unacceptable usage shall lead to disciplinary action.

3.24. The JMBGRP shall implement a comprehensive framework for the management of technical vulnerabilities within our network security policy. This includes regular vulnerability assessments, prompt application of patches and updates, and continuous monitoring to swiftly identify and address potential security risks.

3.25. The JMBGRP shall enforce stringent controls for information transfer within the network security policy. This encompasses the use of secure channels, encryption protocols, and access restrictions to safeguard sensitive data during transmission.

4. Procedure

This procedure has been structured to address various aspects of logical access on JMBGRP's network and the corresponding security measures / roles which need to be considered for creating

a secure access environment. The areas covered in this procedure include:

4.1. Induction of New Systems

4.2. Security of System Documentation and Configuration files

4.3. Equipment identification in networks

4.4. Access control

4.5. User creation

4.6. Hardening of Systems

4.7. Access List Review

4.8. Clock synchronization

4.9. Terminal Timeout

4.10. Patch Management

4.11. Use of systems utilities and other utility software

4.12. Performance and System Monitoring

4.13. Log Management

4.14. Incident Management

4.15. Exceptional logs

4.16. Security from malicious code

4.17. Anti-Virus Management

4.18. Maintenance of Systems

4.19. Network Infrastructure Security Controls

4.20. Network Management

4.21. Network Routing Control

4.22. Local Area Network (LAN) & Wide Area Network (WAN) Management

4.23. Wireless LAN Access Management

4.24. Firewall Management

4.25. Remote Diagnostics and Configuration ports

4.1. Induction of New Systems

4.1.1. JMBGRP IT Team shall define and document the specifications for hardware and software of a system based on purpose for which the system is used, applications to be run on it and the performance and capacity requirements as per the business needs.

4.1.2. Before induction of the system, the JMBGRP IT Team shall ensure that the hardware and

software configurations meet the specifications of JMBGRP's business requirement.

4.1.3. JMBGRP IT shall prepare a System Checklist which includes the below mentioned, and they shall carry out induction and maintenance as per the System Checklist

4.1.3.1. Physical access control required.

4.1.3.2. Logical name of the system (i.e. name stored in the system).

4.1.3.3. Physical name of system (i.e. name in the asset inventory).

4.1.3.4. Account Policy

4.1.3.5. Account Lock out Policy.

4.1.3.6. General System Settings

4.1.3.7. Recommended Software

4.1.3.8. Administrator and user groups to be created.

4.1.3.9. Log Details and Event and Security Settings

4.1.3.10. User rights assignment

4.1.3.11. Security Options

4.1.3.12. Protection against malicious code (Anti –Virus, Firewall, Spy ware)

4.1.3.13. Operating system patches, Service packs to be applied.

4.1.4. Services details, but not restricted to like internet access, application access, and VPN access.

4.1.5. Systems deployed shall have the JMBGRP baseline security configurations deployed before the systems are introduced in the live environment.

4.1.6. The JMBGRP IT shall periodically update the System Checklist to address new vulnerabilities to the systems based on the inputs from the Information Security Team and as provided by the equipment/software supplier. The Head- Security Team shall review the checklists before they are approved by the Information Security Team.

4.1.7. When operating systems are changed, business critical applications shall be

reviewed and tested by Application Management Teams under the respective program managers to ensure that there is no adverse impact on JMBGRP's operations and security. Change Control Policy and Procedure shall be adhered to while doing so.

4.1.8. For any third-party applications which are to be deployed on JMBGRP's systems, the Program Managers shall conduct impact analysis of the proposed change and also procure necessary product certifications from the supplier to ensure veracity of the stability of the product before deployment.

4.1.9. Only after the new operating system has been checked and necessary change control formalities have been completed, then the new system shall be rolled out.

4.1.10. A final activity report shall be logged before the closure of the activity.

4.1.11. User acceptance testing shall also be carried out to check the final version to be installed in the live environment.

4.1.12. The inventory nomenclature as promulgated by the Inventory Management Procedure shall be used in the labeling process.

4.1.13. The concerned Personnel and System Administrator shall label the asset as per a standard naming convention.

4.2. Security of System Documentation and Configuration files

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

4.2.2. 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 specified in Risk Management Methodology.

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

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

4.2.5. Any exceptions or deviations shall be raised through service request in the JMBITassist portal.

4.2.6. Access rights to the machine where system documentation is stored shall be provided to authorize personnel JMBGRP IT.

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

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

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

4.2.10. All system documentation shall be stored on a document management system.

4.2.11. We are following defined and approved backup with reference mechanism to take timely backup of critical system.

43. Equipment identification in networks

4.3.1. All the network devices, desktops and laptops shall be brought onto a single domain and active directory. Those devices and machines which continue to remain as a part of the work group shall be brought onto the domain in phased manner by the Infrastructure Team or exception shall be raised with appropriate justification. This control shall be applicable for all employees of JMBGRP, permitted third parties who have been given access rights to JMBGRP network. This mechanism shall be applicable for LAN / WAN connections and Remote Connections.

4.3.2. Identification of legitimate and rogue devices shall be established through the network access control management system. Identification shall be done based on assigned MAC ID or IP addresses.

4.3.3. Port security shall be enabled. All unused ports shall be disabled.

4.3.4. A suitable tool shall be deployed to check for un-authorized network access.

4.3.5. 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.

4.4. Access control

4.4.1. Refer to JMBGRP ISMS Access Control Policy for Logical access

4.5. Hardening of Systems

4.5.1. The Information Security Team shall be responsible for preparing of the Hardening Checklists for servers, switches, desktops, core routers, core switches and Wireless devices. The JMBGRP IT shall deploy these checklists.

4.5.2. The JMBGRP IT 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 JMBGRP IT.

4.5.3. The JMBGRP IT Team shall identify the patches required to be applied. In case of servers the deployment shall be through the Information Security Team.

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

4.5.5. Access to system files on servers, routers, switches and firewalls.

4.5.6. The JMBGRP 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 Security In-charge as per business requirement.

4.5.7. The Information Security Team shall periodically conduct hardening activity and submit IT-Team report to the JMBGRP IT 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 half yearly basis or when a new system is inducted into the network.

4.5.8. Environment specific hardening documents shall be prepared. (E.g. Web-server/ Mail server/ Application Database server) and different operating systems like Windows/ Linux/ UNIX as the case may be.

4.5.9. A tool may be applied to Manage configuration using Group Policy for domain joined system, Non-Domain connected system done manually. This tool shall also have remediation capabilities to ensure corrective action is taken without manual intervention.

4.5.10. For all Confidential and critical systems, hardening activity sign off shall be provided by HOD IT.

4.5.11. For all general systems hardening activity sign off shall be provided by Network Team Lead/Manager.

46. Network Device Access List Rule Review (ACL) – For Policy Devices (Managed Switches, Routers and Firewalls)

4.6.1. JMBGRP IT shall prepare a base line ACL documentation for each category of the network device.

4.6.2. All network devices shall be subjected to a quarterly review of their access lists with reference to the baseline list.

4.6.3. The baseline list shall also be revised when changes are done to the device IOS, devices are refreshed.

4.6.4. Default settings shall be changed on new devices.

4.6.5. For all general systems hardening activity sign off shall be provided by Head Network Team.

4.6.6. For all Confidential systems hardening activity sign off shall be provided by Head Network Team, Chief Tech Support and Network Architecture.

4.8. Clock synchronization

4.8.1. System/Network Administrators of all servers and network devices shall synchronize the clocks of servers/network devices with the time server. The process is outlined below

4.8.1.1. System/Network administrators shall follow processes to maintain server time in sync with IST time

4.8.1.2. Open Date and Time window and check current time of the Server.

4.9. Terminal Timeout

4.9.1. 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 each application, it shall be defined as per business sign off.

4.10. Patch Management

4.10.1. JMBGRP IT shall ensure that current OS patches are identified, tested before they are deployed.

4.10.2. JMBGRP IT shall test the patches on a test system before applying them to live system. In case testing is not possible, the System Administrator shall take permission from the Information Security Team to apply it directly to the live server and network devices. JMBGRP IT shall ensure proper data and configuration backup before applying the patches.

4.10.3. All Critical and Confidential servers, devices and appliances shall be patched on a priority basis by Network Team followed by the rest.

4.10.4. The relevant patches shall be installed on the systems through WSUS or patch management system.

4.10.5. Patch deployment shall happen in the night after closure of office hours and or business hours or in case of urgency, it will be performed with required approval.

4.10.6. 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.

4.11. Use of systems utilities and other utility software

4.11.1. The access to systems utilities shall be restricted as per the Access Control Policy and Procedure. Users shall not be given access to the systems utilities.

4.11.2. 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.

4.12. Performance and System Monitoring

4.12.1. Operating System shall be configured as per Hardening Checklist. To generate detailed audit logs for System and Security events automated tools shall be used. These logs shall be appropriately backed up. Procedure for review of logs in order to monitor activities at the operating system level and identify any possible security violations shall be followed as per Network Security Policy and Procedure by System Administrators taking in account the OS, criticality and risk assessment of the installation. Where possible there shall be an automated procedure to ensure that these logs are reviewed on a regular basis. Logs shall be retained for as per the Log specification Form in Network Security Procedure. Any deviations or observations found shall be immediately reported to the JMBGRP IT.

4.13. Log Management

4.13.1. End User Computing Team shall identify the logs to be monitored. For critical device log identified, he shall record 'Log Management' which shall include

4.13.1.1. Name of the log,

4.13.1.2. IT system on which the log is required to be enabled,

4.13.1.3. Contents of the log,

4.13.1.4. Frequency of logging,

4.13.1.5. Duration of logging,

4.13.1.6. Log rotation frequency (Log rotation refers to regular moving of an existing log file to some other filename and starting fresh with an empty log file),

4.13.1.7. Person responsible for monitoring the log,

4.13.1.8. Frequency of monitoring,

4.13.1.9. Format, medium, frequency and intended recipients of Log Monitoring Report,

4.13.1.10. Access control matrix for access to logs.

4.13.2. Log Backup

4.13.2.1. Logs of Critical systems and network shall be backed up as per business need.

the appliance on an external media such as tapes. Weekly backup media shall be rotated every month.

4.13.3. Log Monitoring

4.13.3.1. All critical and confidential devices (Firewall, Routers, Switches and Servers) and applications (AD, Notes, SAP, Systems deployed for Manufacturing Environment) shall have their audit and event log functions enabled.

4.13.3.1.1. JMBGRP Network Team Members who are designated to monitor a log shall monitor the log as per the frequency mentioned in the 'Log Specification'

4.13.3.1.2. A suitable Platform shall be deployed for monitoring and logging security incidents. The Platform shall perform incident correlation to provide insights to the network security team. All critical and confidential network devices, servers and applications shall be monitored.

4.13.3.1.3. A separate application monitoring platform shall be considered to monitor application parameter monitoring and performance so as to ensure optimal utilization of application resources and also ensuring optimal availability.

4.13.3.1.4. Administrator, Privilege User Logs shall be monitored for all critical and confidential systems and applications.

4.13.3.1.5. All logs emanating from remote access shall also be monitored.

4.13.3.1.6. Log information is protected in the system using access control mechanism.

4.13.3.1.7. If Log is backed up in media, it is controlled through physical access control mechanism. Logs on media shall be encrypted.

4.13.3.1.8. Only authorized IT Network Security Team Members

shall have the rights to see the logs.

4.13.3.1.9. The System Executive shall report the findings of the log monitoring in a Log Monitoring Report. Format, medium, frequency and intended recipients of the Log Monitoring Report shall be as per the prescription in the 'Log Specification'.

4.13.3.1.10 Logs are maintained based on the storage capacity defined. Logs are overwritten automatically

4.14. Maintenance of Systems

4.14.1. JMBGRP IT shall ensure that the backup of the data is taken before any system maintenance activity for servers, routers, switches and appliances are performed.

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

4.14.3. 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.

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

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

4.14.4.2. 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.

4.14.4.3. A disk quota shall be assigned to the file system for each user, where the user's

4.14.4.4. home directories are kept.

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

4.14.4.6. 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 HOD JMBGRP IT in consultation

with the application\server owner by mail and or through the OCR (On Call Request) and after changes it should be regularized in change request.

4.15. Network Infrastructure Security Controls

4.15.1. Complete architecture of the network shall be documented by the Network Administration Team for all the locations of JMBGRP shall be reviewed before seeking approval from the Head IT Infrastructure. Any subsequent changes to the network shall also be documented and approved. Version control for the same shall be maintained.

4.15.2. DMZ (Demilitarized Zone) shall be created to segregate internal and external networks with all connections getting routed through this firewall.

4.15.3. Network devices administration shall be restricted to authorized staff only.

4.15.4. Network Administrator shall ensure that all network devices on the network are monitored for up-time and bandwidth. E.g., Routers, Switches, Wi-Fi Access Points.

4.15.5. V-LANs shall be implemented to segregate critical business departments so that inter departmental system access shall be restricted unless it is approved by the Infrastructure Team and the concerned business group/department purely on business requirement. Access in this case shall be controlled and access lists shall be maintained and reviewed on a periodic basis (once every 12 months).

4.15.6. Servers/network devices shall be on a different V-LAN/DMZ.

4.15.7. V-LAN shall be monitored through the deployment of a suitable monitoring tool for broadcasts or any abnormal traffic.

4.15.8. Guests connecting to JMBGRP network shall be on a different VLAN with zero privileges.

4.15.9. Deploy Email and Web Content Filtering Software for protection against spam and viruses.

4.15.10. Deploy a suitable Data Leakage Management or Data Leakage Prevention or Information Rights management tool for data protection when stationary, in transit or when it needs to be archived.

4.15.11. Internal and external vulnerability assessment and penetration testing, device configuration reviews, access lists reviews shall be performed every six months.

4.15.12. Network Security Architecture Review (NSAR) assignment shall be performed, once every year or when significant changes are done to the networking environment.

4.16. Network Management

4.16.1. Network Administrators shall change the factory default configuration and passwords (as per password Security Policy) of all network device and security setting would be enabled on all network devices.

4.16.2. Infrastructure Team shall maintain an updated list of all the IP Addresses assigned throughout the network. The IP Address schema shall be approved by Infrastructure Team.

4.16.3. Configuration Management – Infrastructure Team shall maintain inventory details and configuration of LAN, WLAN and WAN equipment.

4.16.4. Secure Password Management – All passwords of network equipment and network management systems shall be changed as per Password Security Procedure.

4.17. Network Routing Control

4.17.1. Access to routers / layer 3 switches shall be done in a secure manner (only SSH) and no telnet. Personnel allowed to access the devices shall be rotated in their duties to prevent long duration of familiarity and possible occurrence of any breach.

4.17.2. Access control lists of routers and layer 3 switches shall be reviewed once every 6 months by the JMBGRP Network Team for critical and confidential devices. Review reports shall be generated and appropriate corrective and preventive action plan shall be created. Reports shall be retained for audit purposes.

4.18. Local Area Network (LAN) & Wide Area Network (WAN)

4.18.1. A dedicated team shall be formed to monitor traffic from the enterprise wide installations of network devices on 24x7 bases using a networking tool.

4.18.2. Incident management process shall be instituted as per the Incident Management Policy and Procedure.

4.18.3. Changes to any devices shall be done as per the Change Management Policy.

4.18.4. The activities of the Third-Party Network Service Providers who have privileged access on the critical machines/devices shall be monitored. JMBGRP shall include the necessary clauses in the agreement to reserve the right to audit the activities of Third Parties.

4.18.5. Assigned Member of the Network Administrators Team shall ensure that proactive monitoring of LAN & WAN links is done for bandwidth utilization and identifying any suspicious traffic through approved tools. If found then the same shall be logged as per Log Monitoring Procedure mentioned below and reported to the Information Security Expert Group.

4.18.6. Assigned Member of the Network Administrators shall ensure that all the LAN & WAN Devices are remotely manageable and shall have an access-controlled management console.

4.18.7. Network Administrators shall ensure that user access to the LAN & WAN resources are authorized and access controlled and shall be based on the approved logical access request. In case of access from public network, the connection shall be encrypted, and strong authentication protocols shall be deployed.

4.18.8. Network Administrators shall ensure that any change in Network Device or IT-Team configuration or implementation of new device is approved by Information Security Expert Group and a record of the same maintained for audit purpose.

4.18.9. Submit a report to the HOD IT on the Bandwidth consumption by segment, number of incidents reported, closed, pending, dependent activity, impact on business and corrective and preventive action plan.

4.18.10. The physical access to premises housing network devices and servers shall be through biometric access and CCTV surveillance shall be deployed.

4.18.11. Servers shall be housed in a dust proof environment in a protected rack. Temperature and Relative Humidity shall be maintained as per manufacturer's recommendations.

4.19. Wireless LAN Access Management

4.19.1. Infrastructure Team shall be responsible for the installation and maintenance of wireless access points.

4.19.2. Ensure that security features on wireless devices are enabled (as embedded security features are disabled by default.)

4.19.3. Use of encryption and logical separation (e.g. Wi-Fi Protection Access - WPA 2 and V-LAN).

4.19.4. Information Security Group shall ensure that unauthorized use of wireless access capabilities shall be prevented through the following measures:

4.19.4.1. Changing security-related default access point settings, such as the Service Set Identifier (SSID) and the IP address.

4.19.4.2. Do not broadcast SSID.

4.19.4.3. Disabling beacons within access points that regularly broadcast the SSID.

4.19.4.4. Change the default admin password and deploying a complex password as per password policy.

4.19.4.5. HTTPS is enabled instead of HTTP for logging into the access point's web configuration page.

4.19.4.6. Disabling services like TELNET and SSH on the Access Points

4.19.4.7. Housing the access points well within the building to prevent unwarranted spillover of the signals outside the premises.

4.19.5. Network Administrator shall enforce 30-minute re-authentication for all users. With every unsuccessful attempt the time will increase exponentially. Refer Password Policy and Procedure.

4.19.6. Network Administration Team shall enable logging of all inbound and outbound activity on the Wireless Access Point to allow auditing of wireless access.

4.19.7. Network Administration Team shall do regular assessments of Wireless LAN to check for Rogue Access Points. Periodic Wireless Security Audit review shall be conducted to ensure that wireless networks are operating as per the security requirements.

4.20. Firewall Management

4.20.1. Firewall shall be installed to segregate the following networks.

4.20.1.1. Internal network and External Public network.

4.20.1.2. Internal network and DMZ

4.21. Information Security Group shall ensure that

4.21.1.1. Firewall is configured to filter packets for correct incoming and outgoing addresses.

4.21.1.2. Only required services are enabled on the firewall.

4.21.1.3. Ports that are vulnerable or not required are disabled on the firewall.

4.21.1.4. Firewall rules are reviewed every six to check for any redundant rules.

4.21.1.5. Firewall logging shall be enabled.

4.21.1.6. Monitoring of Firewall logs shall comply with the clauses in Log Monitoring Procedure mentioned below.

4.21.1.7. Reporting and investigation of any incidents shall be as mentioned in Incident Management Policy and Procedure.

4.21.1.8. Firewall configuration and log files are backed up as per Backup, Restoration and Media Handling Policy and Procedure.

4.21.1.9. Web Application Firewall shall be considered for blocking web related threats.

4.22. Head IT Infrastructure shall approve changes to the firewall configuration after assessing the reason(s) for change.

4.23. The changes are documented and the necessary roll back procedures are decided, in case of failure after change.

4.24. Internal and external vulnerability assessment is performed on the firewall on an ongoing basis to test for known software flaws and weaknesses.

4.25. Network Fire Wall Administrators shall subscribe to the firewall vendor's security bulletins.

4.26. Configuration Reviews and Rule Reviews shall be done once every quarter and identified vulnerabilities closed.

4.27. Management of Technical Vulnerabilities

4.27.1. Identify technical vulnerabilities within information systems using scanning tools and threat intelligence.

4.27.2. Conduct regular vulnerability assessments to evaluate exposure and risk.

4.27.3. Prioritize vulnerabilities based on severity and potential impact.

4.27.4. Establish patch management processes for timely remediation.

4.27.5. Implement compensating controls for vulnerabilities that cannot be immediately patched.

4.27.6. Develop an incident response plan for addressing security incidents related to vulnerabilities.

4.27.7. Continuously monitor systems for new vulnerabilities using detection systems and threat intelligence.

4.27.8. Provide security awareness training to educate employees on identifying and reporting vulnerabilities.

4.27.9. Maintain documentation of vulnerability assessments, remediation efforts, and ongoing risk management activities.

4.27.10. Regularly review and improve the vulnerability management process based on feedback and lessons learned.

4.28. Information Transfer Process

4.28.1. Conduct a thorough assessment of existing information transfer mechanisms and associated risks.

4.28.2. Identify all types of data transfer facilities within the organization and those involving external parties.

4.28.3. Review current policies, procedures, and agreements related to data transfer to understand their effectiveness and compliance with regulatory requirements.

4.28.4. Develop comprehensive information transfer rules, procedures, or agreements to govern all data transfer activities.

4.28.5. Specify protocols, standards, and responsibilities for secure information transfer, ensuring clarity and alignment with organizational goals.

4.28.6. Include provisions for different types of transfer facilities, such as internal networks, cloud services, and third-party connections.

4.28.7. Implement encryption mechanisms to safeguard data integrity and confidentiality during transit.

4.28.8. Deploy secure communication protocols, such as TLS/SSL, to establish encrypted connections for data transfer.

4.28.9. Configure access controls and authentication mechanisms to restrict unauthorized access to sensitive information during transfer

4.28.10. Define a clear retention policy outlining the duration and conditions under which data can be retained during transfer.

4.28.11. Ensure compliance with legal, regulatory, and industry requirements while considering operational needs and data security considerations.

4.28.12. Establish procedures for secure data disposal once retention periods expire to minimize data exposure and mitigate risks.

4.28.13. Implement robust monitoring mechanisms to track data transfer activities and detect anomalies or unauthorized access attempts.

5. Responsibilities

The responsibility for implementing this policy is with the following personnel:

5.1. IT Administrator and Team:

5.1.1. Label and issue the media.

5.1.2. Review the status logs of the backup activity.

5.1.3. Inform the application owners/HOD whenever there is a failure of data backup.

5.1.4. Ensure proper configuration of the backup system.

5.1.5. Backup data in accordance with the schedule.

5.1.6. Maintain / Review restoration drill schedules and execute the same.

5.1.7. Restore data whenever requested and take a sign off from the requester of successful restoration.

5.1.8. Maintain accounting of issued media.

5.1.9. Assign the responsibilities of backup to the IT Administrator.

5.1.10. Review the backup request and assign the task to IT Administrator.

5.1.11. Random review of the backup/restoration logs and media. Review media issue register.

5.1.12. Approve direct restoration on live server in case of data loss.

5.1.13. Approve disposal of media.

5.1.14. Manage offsite backup process.

5.1.15. Ensure Information Security Team Audit-Team the backup process on-site and offsite.

5.2. HOD, application owners and Users as the case may be:

5.2.1. Give information to IT Team about the data to be backed up, the frequency of backups etc. taking into consideration the criticality of information.

5.2.2. Ensure backups are taken for their business critical data.

5.2.3. Request restoration in case of loss to data. CONFIDENTIAL business data and adhere to this procedure. Non-compliance to this could result in disciplinary action as per the code of conduct of the organization.

5.2.4. While restoring the files and directories, it shall be ensured that access permissions are not changed after restoration is complete.

6. Enforcement

6.1. Any employee found to have violated this procedure shall be subjected to disciplinary action as per JMBGRP Code of Conduct Procedure.

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

7. Metrics

7.1. Metrics shall be measured by IT Team and shall be reported to respective HoDs every quarter.

7.2. The periodicity of reporting shall be once in a quarter and shall include, but not limited to:

7.2.1. Number of times restoration has failed for Critical and Confidential assets

7.2.2. Number of times data was lost on account of back up not being taken.

7.2.3. Number of times media was lost on account of it not being entered into the register before removal.

7.2.4. Number of times back up media was lost in transit/damaged/stolen.

7.2.5. Media wise issues during the backup procedure.

7.2.6. Number of times scheduled back up and restoration has not happened.

7.2.7. Media destroyed without any record.

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 the Information Security Policy and Procedures may have to be allowed at the time of implementation of these policies and procedures or at the time of making any updating to this document or after implementation on an ad hoc basis based on business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.

8.3. All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception Form and sign-off on the same shall be maintained including ad-hoc requests.

8.4. 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 Backup, Restoration and Media Handling 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 Backup and Restoration 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 Backup and Restoration policy and procedure document shall not be considered as implied in any manner.

9.2. For any clarifications related to this Backup and Restoration policy and procedure document with respect to IT-Team interpretation, applicability, and implementation, please raise a request ticketing Tool.

10. References

ISO 27001:2022 - A.8.15, A.8.16, A.8.17, A.8.19, A.8.34, A.8.20, A.8.21, A.8.22, A.5.14, A.5.35, A.8