Information Security Management System

Log Management Policy & Procedure

Document no. JMBGRP/ISMS/Pol-LM

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document to provide a log management framework to capture improper behavior of information systems, to foster accountability, and to improve systems management for better availability of IT Systems.	
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	25.08.2023	Manish Jaiswal (Group CTO)	Changes done for logs monitoring to be enabled	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: “Procedure, Responsibilities”	

Contents

Purpose

The purpose of this policy is to provide a log management framework to capture improper behavior of information systems, to foster accountability, and to improve systems management for better availability of IT Systems.

Scope

J.M Baxi Group and Scoped Locations

Employees of JMBGRP's and all personnel using the information technology resources of JMBGRP's are in scope. This includes external parties like contractors, vendors, third party service provides, business associates and any temporary employees, customers and trainees who have been granted access to the JMBGRP's computer network, which includes, LAN, WAN, Dial–Up Access and data communication equipment and facilities.

Policy Statement

- JMBGRP should ensure development and implementation of procedures and controls related to monitoring of technology infrastructure to detect deviations from access control policy and recording events to provide evidence in case of incidents.
- All the systems should be time synchronized.
- Logging should be enabled for all devices, servers, end point systems and applications.
- Audit trails should be identified and maintained for business-critical systems and applications.
- Regular log analysis should be conducted on identified servers, devices and laptops.
- Logs should be backed up for audit purposes.

Procedure

1.1 Clock synchronization

1.1.1 System Administrator shall define one system as a clock reference for all and it should take reference clock from internet through reliable source.

1.1.2 System Administrator shall set the time of the 'time server' to Indian Standard Time (IST).

1.1.3 Configure all other information systems as NTP to take the reference clock.

1.1.4 IT Admin shall be responsible for monitoring logs.

1.2 Log identification for monitoring

1.2.1 The IT Admin shall identify the logs to be monitored and the 'Log Specification' shall include.

1.2.1.1 Source of Log

1.2.1.2 Types of Logs (Security, System, Application)

1.2.1.3 Frequency of logging

1.2.1.4 Frequency of monitoring

1.2.1.5 Log retention period

1.3 Log Enabling

1.3.1 The System Administrator shall enable the logs as per the details mentioned in the 'Log Specification'.

1.3.2 Adequate size for the log files shall be set.

1.4 Log Backup and Rotation

1.4.1 A location specific log server shall be used to store logs of all systems.

1.4.2 System Administrator shall ensure that the logs of the information system are maintained for critical server.

1.5 Log Monitoring

1.5.1 System Administrator shall monitor a log as per the frequency mentioned in the 'Log Specification'.

1.5.2 The System Administrator shall report the findings of the log monitoring in a Log Monitoring Report.

1.6 Log Analysis

1.6.1 Logs generated shall be analyzed on periodic intervals by system administrator or persons authorized by IT Team.

1.6.2 Logs analysis report shall be submitted to the Head IT on Quarterly basis.

1.7 Log Disabling and Deletion

1.7.1 The logs on the systems should not be deactivated. If these need to be deactivated for some reason the exception signoff process should be followed.

1.7.2 Access to delete logs shall not be provided to anyone.

1.8 Administrator Logs monitoring

1.8.1 Administrator's activity logs shall be captured in the AD server where the logs cannot be modified or deleted.

1.8.2 The Administrator's activity logs shall be accessible by the IT departments and monitoring of the logs shall be with Infra Team.

1.9 Exceptional Logs

1.9.1 There are situations where particular events are required to be tracked for specific reasons (e.g., suspected fraudulent behavior). In such a situation, Process Head, who require logging of events, shall send a request to the system Admin. The same shall be reviewed by the System Admin & inform the same to Head-IT & Chief Information Security Officer.

1.10 Guidelines

1.10.1 Logs to monitor unauthorized access shall be enabled on Infrastructure Servers, Production systems.

1.10.2 The following logs shall be considered for monitoring of anomalous behavior

1.10.3 Network logs such as Access Points, Router logs, Switch logs, Firewall logs, IPS logs.

1.10.3.1 Application Server logs, Web server logs, Mail server logs.

1.10.3.2 Database Server logs (User activity, Objects accessed, new tables/ Objects created)

1.10.3.3 Operating System logs such kernel messages, private authentication, mail, emergency messages and boot logs for UNIX/Sun Solaris (but not limited to).

1.11 Following events to be monitored

1.11.1 Administrative account activities

1.11.2 System events

1.11.3 Application events

1.11.4 Security related events

1.11.5 Remote access to the critical hosts

1.11.6 Console alerts or messages

1.11.7 User/group creations and deletions

1.11.8 Unauthorized access

1.11.9 Repeat Attack-Login Source & Target (Application, Firewall, Routers, Switches etc.)

1.11.10 Attacks and Infections Detected at the Host Level

1.11.11 Attacks from Unknown/Untrusted Sources

1.11.12 High Threat targeting vulnerable assets

1.11.13 Possible outbreak – excessive connections

1.11.14 Possible outbreak- multiple infected hosted detected on the same subnet

1.11.15 Access reports to core infrastructure assets

1.12 Logs shall be enabled for at least the following events in case of Operating Systems and Databases:

1.12.1 Record of successful / unsuccessful system access attempts

1.12.2 Record successful / unsuccessful account management attempts.

1.12.3 Record attempts to modify logs.

1.13 Logs shall be retained as per the classifications outlined below. Retention periods may vary based on business requirements and access frequency.

Windows Servers	One year
Linux Servers	One year
Switches	One year
Routers	One year
Firewall/IPS	One year
WIFI Controller	One year
CCTV in server room	One year
Card Reader in server room	One year
Anti-Virus	One year
Applications	One year

1.14 Log Monitoring

Windows Servers	Incident Based
Linux Servers	Incident Based
Switches	Incident Based
Routers	Incident Based
Firewall	Real Time Monitoring
WIFI Controller	Real Time Monitoring
Card Reader In Server room	Incident Based
Anti-Virus	Real Time Monitoring
Applications	Real Time Monitoring

Responsibilities

The responsibilities lies with the following personnel:

- Security In-charge
  - Review log monitoring process at least once month
- System administrator
  - Synchronize server clock with 'time server.'
  - Enable / disable logs as per procedure.
  - Monitor logging process.
  - Ensure that logs are copied on central log server.
  - Ensure backup of central log server

- Prepare and distribute Log monitoring report every month.
- Review the Log Monitoring report daily.
- Review the exceptional logs.

Enforcement:

- This policy and procedure is applicable for all the employees of the company who have access to and use the information assets and IT assets as listed in the Information Asset Classification sheet which have been created for all the departments. Any violation shall be dealt with in accordance with the disciplinary action process as laid down in the Code of Conduct.
- Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the rights to alter or amend any clause in this document at any time as per it-team discretion.

Metrics

- The metrics shall be measured by the IT Team under the Information Security Manager.
- The periodicity of reporting shall be once a year.
- The metrics shall be monitored are as given under:
  - Number of critical devices covered under Log Management
  - Number of anomalies found during monitoring.
  - Number of cases reported to ISM.
  - Corrective actions/ if any.

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 this Security Policy and Procedures shall be allowed at the time of implementation of this policy and procedures or at the time of making any updation to this document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which shall 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 it-team interpretation, applicability and implementation, please raise a request in Ticketing Tool.

References:

- Control Objectives: A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4