Information Security Management System

Web Access Policy

Document No. – JMBGRP/ISMS/POL-WA

Version_v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	Web access/ Internet usage management	
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)	Document reviewed. Modification done to "13. Reference to ISO 27001:2022"	
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: "Scope, Procedure, Responsibilities, Enforcement"	

Contents

1. Purpose 4
2. Scope 4
3. Policy 5
4. Procedure 5
5. Responsibilities 9
6. Enforcement 10
7. Metrics 10
8. Exceptions 11
9. Disclaimer 11
10. Reference to JMBGRP Policy and Procedures 11
11. Reference to ISO 27001:2022 12

1. Purpose

1.1. This document articulates the policy for internet usage and steps involved in safe and secure usage of internet for business use. So also, it enlists the best practices which need to be followed and practices which are not permitted by J M Baxi Group (JMBGRP).

2. Scope

This policy is applicable for all the employees in JMBGRP at all corporate offices and all the plant locations as well as the Third-Party Vendors.

3. Policy

3.1. JMBGRP encourages the use of Internet to expedite the business work process. But internet connectivity presents the company with new risks that shall be addressed to safeguard the facility's vital information assets.

3.2. Internet facility shall be provided to employees on a need-based basis through a formal process of approval.

3.3. There shall be formal mechanism to monitor, block and check the content which has been accessed by employees for employees accessing the internet from within the JMBGRP network or from their mobile devices, laptops, phones when outside the JMBGRP network.

3.4. Employees using Internet as provided by JMBGRP on the company's assets shall always ensure that usage, shall in no way compromise or expose the Network and or Assets of JMBGRP to external threats.

3.5. JMBGRP reserves the right to revoke or suspend internet use, should a business situation warrant such a step.

4. Procedure

4.1 The procedure on Internet usage shall cover the following areas:

4.1.1 Granting Access to the Internet

4.1.2 Controlling Internet Access

4.1.3 Usage of the Internet

4.1.4 Monitoring of Usage

4.1.5 Information Handling

4.2 Granting Access to the Internet

4.2.1 Access to the Internet will be provided to employees for business use after authorization from the HOD. Once approved, the necessary access rights will be granted to the user for browsing and the same will be communicated to the user.

4.2.2 Internet access is given to specific users and these rights shall not be transferred or extended to others.

4.2.3 Please refer to the Ticketing Tool for access to Internet.

4.2.4 Access shall be reviewed on a periodic basis and shall be revoked, if not required.

4.2.5 IT Team shall maintain a list of users who are having internet access to their respective HODs on a monthly basis for review and concurrence.

4.3 Controlling Internet Access

4.3.1 Internet websites are categorized according to their content. To enforce safe browsing, various categories of web sites will be blocked at the company firewalls through Web Content Filtering.

4.3.2 Connectivity shall only be through proxy server and company reserves every right to monitor, examine, block or delete any/all incoming or outgoing Internet connections on the company's network.

4.3.3 Users shall not use personal modem / wireless data card / any other media to access internet while being connected to JMBGRP's Corporate LAN.

4.3.4 Concerned IT Team shall review the categories as per business needs and shall include / exclude permissible content as per business need and perceived threats.

Blocked		Allowed
Category 1	Category 2	Category 3
Adult	Entertainment	Business
Crime	Job Search	Computing IT
Malicious	Investment Sites	Search Sites
Violence	Game	E-banking
Government Blocking List	Matrimonial	News (without Video)
Swimsuit Lingerie	Personal Belief, Culture	Health
SPAM	Clubs and societies	
Gambling	Chat	
Drugs and alcohol	Music & Video	
Dating	Sports	
Tor Network	Politics	
Torrent Websites	Travel-Tourism	
Personal VPN	Shopping	
	Other Business Email accounts	
	Social Media Websites	
If any useful link is wrongly classified, please inform Security In-charge through Ticketing Portal		

4.4 Usage of the Internet

4.4.1 All Internet data that is composed, transmitted and/or received by JMBGRP's computer systems is considered to belong to JMBGRP and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons.

4.4.2 Internet access is provided for official business purposes. Occasional personal use outside working hours is permitted, but prolonged personal use is not allowed; such usage will be treated as violation and may result in disciplinary action.

4.4.3 No information relating to the organization may be posted onto the Internet without written permission from Senior Management. In case of doubt about material that may be posted Corporate Communications should be contacted. Note that information that is confidential, or any other information that may damage the reputation of the company, shall never be posted onto the Internet.

4.4.4 The Internet shall not be used to create legal or contractual obligations, such as ordering goods or services, unless it is part of normal business activities and has been authorized by Senior Management.

4.4.5 Material shall not be posted or downloaded which is obscene, malicious, threatening, hostile, abusive, vulgar, defamatory, profane, and unethical or contains derogatory remarks relating to gender, race, religion, color, national/ethnic origin, marital status, age, physical/mental disability, medical condition or sexual orientation, or anything else objectionable and not abiding by the law.

4.4.6 Therefore, employees shall not share or solicit to share, exchange, create, store distribute information either in digital or non-digital form which may cause slander and or attempt to slander, defame, disrespect individual employees, employee groups, religious or social values as professed by employees within JMBGRP, allude to or fuel development of acrimony and or discontent amongst employees and also violate the Indian Law in any manner.

4.4.7 Official company information shall not be revealed in blogs, message boards, personal web sites amongst, social media, networking sites.

4.4.8 Employees shall not reveal official, personal or organizational details to any website which is not relevant to company business (e.g. when completing forms to subscribe to newsletters) and do not use internal company passwords on Internet sites.

4.4.9 Internet postings are subject to the same legal rules that cover printed material, be it copyright protection, libel, criminal conduct, fraud etc. Internet postings shall therefore be proper, appropriate and factually correct.

4.4.10 Responsibility of Internet activities will rest with the user. The company does not accept liability for any personal damage or loss incurred as a result of Internet activity.

4.4.11 Any document being sent through the Internet goes into the public domain and therefore users should act accordingly regarding company confidentiality policies. If any confidential information has to be sent, it should be sent in an encrypted form by saving the document with a password.

4.4.12 Files for private use such as music, videos, photographs amongst others, shall not be downloaded or uploaded.

4.4.13 Users shall not download very large files during normal office hours.

4.4.14 Using the Internet for listening to the radio is not permitted since such activity tends to congest the data pipe thereby hampering end user experience.

4.4.15 Social networking sites such as Facebook amongst others shall not be used during office hours unless for legitimate business purposes. Even when used out of office hours or from home, it is prohibited to publish any official information relating to the company on any such public sites.

4.4.16 Access to public mail sites, chat engines, social networking sites and use IP messengers, P2P tools shall not be permitted. For a justifiable business reason, if usage is mandated and necessary then it shall be done through a proxy. The HOD shall take complete onus and responsibility of internet usage by the employees in the department.

4.5 Monitoring of Usage

4.5.1 The company shall monitor Internet usage of users without prior notice. Monitoring will be performed in accordance with company policy and national laws. If there is evidence that a user is not adhering to the requirements set out in this policy, the company reserves the right to take disciplinary action.

4.5.2 The company reserves the right to block or allow certain sites without prior notice and may withdraw access to the Internet for individuals if deemed necessary.

4.6 Information Handling

4.6.1 Information handling during Internet activities shall be done in accordance with the handling guidelines for respective class of information.

4.6.2 No critical and confidential information shall be shared in any manner on the internet.

4.6.3 Public data storage sites such as Dropbox, One Drive are not permitted and even use of file sharing sites is not permitted.

4.6.4 Responsibilities

4.1. The responsibilities lie with the following personnel:

4.1.1. Employees/Users:

4.1.1.1. To protect information assets and follow the Web Access policy and procedures.

4.1.1.2. To report breaches or violations.

4.1.2. IT Network Team:

4.1.2.1. To enforce the Internet security controls applicable to IT Systems.

4.1.2.2. Proactively monitor the effectiveness of the controls.

4.1.2.3. Report content violations, upload and download statistics and other violations.

4.1.3. Departmental Managers, Chiefs and Heads:

4.1.3.1. Provide approval for internet access.

4.1.3.2. Facilitate disciplinary action should a violation be reported.

5. Enforcement

5.1. This policy and procedure are 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 in accordance with the disciplinary action process as laid down in the Code of Conduct.

5.2. 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 document at any time as per its discretion.

6. Metrics

6.1. The metrics shall be generated by the IT Team and reported to Business Security In-charge, Head of department and Security In-charge on a bi-annually basis.

6.2. The metrics shall be measured on bi-annually basis and reported. The points include as given below, but not restricted to.

7.2.1 Number of attempts to download non permissible sites.

7.2.2 Number of incidents on unacceptable usage of Internet.

7.2.3 Number of failed attempts to log into provisioned services.

7.2.4 Consumption of bandwidth for official and personal use.

7.2.5 Number of users uploading and downloading data by size and periodicity.

7. Exceptions

7.1. 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 reason existing at any point of time.

7.2. 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 updates 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.

7.3. All exception requests shall be submitted by respective DI to HoDs and ISOs. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester. [Refer: Annexure – A: Exception From]

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

8. Disclaimer

8.1. J M Baxi Group (JMBGRP) reserves all rights and is the exclusive owner of all intellectual property rights over this Internet 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 Internet 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 Internet policy and procedure document shall not be considered as implied in any manner.

8.2. For any clarifications related to this Internet policy and procedure document with respect to its interpretation, applicability and implementation, please raise a ticket in ticketing Tool.

9. Reference to JMBGRP Policy and Procedures

9.1. Network Security Policy

9.2. Remote Access Policy

9.3. Privilege Management Procedure

9.4. Procedure for Mobile Computing Equipment

10. Reference to ISO 27001:2022

Control Objective: A.5.10, A.5.14, A.8.15, A.5.16, A.5.18, A.8.19, A.6.8,