IT Infra Cybersecurity Policy
JBM Group

DOCUMENT INFORMATION

Rev. No	Release date	Description of change	Prepared by	Approved by
00	01.08.2024	IT Infra Cybersecurity Policy Controlled & Copy issued	Mr. Sivagurunathan Y (Senior Manager Information Security)	Mr. Lalit Kaushik (General Manager Information Security)
01	11.01.2025	Updated as per VCA pre audit review feedback	Mr. Sivagurunathan Y (Senior Manager Information Security)	Mr. Lalit Kaushik (General Manager Information Security)
02	04.03.2025	Updated as per VCA pre audit review feedback	Mr. Sivagurunathan Y (Senior Manager Information Security)	Mr. Lalit Kaushik (General Manager Information Security)

CONTENTS

Acceptable Use Policy

1. Overview

Information Security (InfoSec) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to JBM Group established culture of openness, trust and integrity. InfoSec is committed to protecting JBM Group employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of JBM Group. These systems are to be used for business purposes inserving the interests of the company and our clients and customers during normal operations.

Effective security is a team effort involving the participation and support of every JBM Group employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at JBM Group. These rules are in place to protect the employee and JBM Group. Inappropriate use exposes JBM Group to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct JBM Group business or interact with internal networks and business systems, whether owned or leased by JBM Group, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at JBM Group and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with JBM Group

4. Policy

4.1 General Use and Ownership

4.1.1 JBM proprietary information stored on electronic and computing devices whether owned or leased by JBM Group, the employee or a third party, remains the sole property of JBM Group. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of JBM Group proprietary information.

4.1.3 You may access, use or share JBM Group proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Individual department head must provide approval to IT team to provide access for department employee towards personal use of Internet/Intranet/Extranet systems.

4.1.5 For security and network maintenance purposes, authorized individuals within JBM Group may monitor equipment, systems and network traffic at any time.

4.1.6 JBM Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that interface with the internal network must adhere to strict access controls based on security requirements. This policy applies to both internal and external users, ensuring that device access is restricted.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Employees are prohibited from utilizing business email address to access social media platforms for personal purposes. The Corporate Communications Department is the only entity authorized to manage and publish official social media content on behalf of the organization.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of JBM Group authorized to engage in any activity that isillegal under local, state, federal or international law while utilizing JBM Group owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities whichfall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.3.1.1 Violations of the rights of any person or company protected by copyright, trade secret, patentor other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by JBM Group.

4.3.1.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted data, and the installation of any copyrighted software for which or the end user does not have anactive license is strictly prohibited.

4.3.1.3 Accessing data, a server or an account for any purpose other than conducting JBM Group Business, even if you have authorized access, is prohibited.

4.3.1.4 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.3.1.5 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, Phishing mails, Ransomware, etc.).

4.3.1.6 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.3.1.7 Using a JBM Group computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

4.3.1.8 Making fraudulent offers of products, items, or services originating from any JBM Group account.

4.3.1.9 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.3.1.10

4.3.1.11 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section,"disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.3.1.12 System (Laptop, Desktop, Server etc.,) scanning or security scanning activities are strictly prohibited unless prior notification is made to the Information Security (InfoSec) team. System scanning may only be conducted by the Plant IT team, and if any unauthorized access or intrusion is detected during the scan, it must be promptly reported to the InfoSec team.

4.3.1.13 Executing any form of network monitoring which will intercept data not intended for the employee’s host unless this activity is a part of the employee's normal job/duty.

4.3.1.14 Circumventing user authentication or security of any host, network or account.

4.3.1.15 Introducing mobile hotspots or similar technology on the JBM Group network.

4.3.1.16 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.3.1.17 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.1.18 Providing information about, or lists of, JBM Group employees to parties outside JBM Group.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

4.3.2.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

4.3.2.2 Any form of harassment via email, fax, telephone or paging, whether through language, frequency,or size of messages.

4.3.2.3 Unauthorized use, or forging, of email header information.

4.3.2.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.3.2.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.3.2.6 Use of unsolicited email originating from within JBM Group's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by JBM Group or connected via JBM Group's network.

4.3.3 Blogging and Social Media

4.3.3.1 Blogging by employees, whether using JBM Group’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of JBM Group’s systems to engage in blogging is acceptable, if it isdone in a professional and responsible manner, does not otherwise violate JBM Group’s policy, is not detrimental to JBM Group’s best interests, and does not interfere with an employee's regular work duties. Blogging from JBM Group’s systems is also subject to monitoring.

4.3.3.2 JBM Group’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any JBM Group confidential or proprietary information, trade secrets orany other material covered by JBM Group’s Confidential Information policy when engaged in blogging.

4.3.3.3 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of JBM Group and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited.

4.3.3.4 Employees may also not attribute personal statements, opinions or beliefs to JBM Group when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of JBM Group Employees assume all risk associated with blogging.

4.3.3.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, JBM Group’s trademarks, logos and any other JBM Group intellectual property may also not be used in connection with any blogging activity.

5. Policy Compliance

5.1 Compliance Measurement

The InfoSec team along with group CIO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the InfoSec team along with the group CIO in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment based on management recommendations.

6. Related Standards, Policies and Processes

- Data Access Process (6.1)
- System Protection from Malware / Virus (6.2)
- Secured Access Policy (6.3)
- Password Policy (6.4)

6.1 Data Access Process

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead tocompromise of very sensitive assets and be a springboard to wider compromise within the organization. Business critical data are stored under common drive with respective user folder names and IT team will ensure to take backup of those critical business data. No users other than IT administrator have administrator rights for any type of operating system (Windows, Linux, Unix etc.,)

6.1.1 Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on oneof JBM Group's networks. Software applications running on JBM Group's networks may require accessto one of the many internal database servers. To access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

6.2 System Protection from Malware / Virus

Recommended processes to prevent virus problems:

- IT Team will always run the supported anti-virus software available from the corporate centralized server and install anti-virus software for all JBM machines (laptops/desktops/servers). Anti-virus updates will happen automatically in background in real time for all the JBM machines (laptops/desktops/servers).
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them byemptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with JBM Group's *AcceptableUse Policy*.
- Never download files from unknown or suspicious sources.
- Anti-virus scanning will happen automatically when any external device (Pen drive, memory card etc.,) is connected with the JBM machines (Laptops/Desktops/Servers).
- Backup of critical applications, SAP, PLM is happening automatically in data centre. The frequency for PLM is weekly full backup, Differential backup daily Database at every 6 hours. For SAP Daily full backup and archive logs happen every 6 hours.
- Run the anti-virus utility to ensure a clean machine, isolate the machine from network and

takesupport from IT team, do not run any applications that could transfer a virus, e.g., email or file sharing, automatic scanning, virus detection, cleaning and quarantine happens every day.

- New viruses are discovered every day. *Automatic Anti-Virus updates* are happening against latest virus signatures.

6.2.1 SAP Disaster Recovery Plan

Contingency Plans

As the process of introducing resilience in SAP Infrastructure, we have set up a Disaster Recovery (DR) site in Bengaluru. This site will enable continuity of business transactions in case any undesired & unexpected disaster happens at primary site in Sify DC Noida. The frequency of conducting DR drills happens 2 times a year.

6.2.2 Removable Media Policy

JBM Group employees are allowed to use pen drives or any external devices in the laptops/desktops. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required when sensitive information is stored on removable media. Moreover, all USB removable media users should provide the USB CONFIDENTIALITY UNDERTAKING form filled and duly signed towards acceptance that any data violations will be fined by JBM Group.

6.3 Secured Access Policy

6.3.1 VPN Access

Approved JBM Group employees authorized may utilize the benefits of VPNs, which are a "usermanaged" service.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to JBM Group internal networks.

2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

5. VPN gateways will be set up and managed by JBM Group network operational groups.

6. All computers connected to JBM Group internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard this includes personal computers.

7. VPN users will be automatically disconnected from JBM Group's network after fifteen minutes

of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.

9. Users of computers that are not JBM Group owned equipment must configure the equipment to comply with JBM Group's VPN and Network policies.

10. By using VPN technology users must understand that their machines are a de facto extension of JBM Group's network, and as such are subject to the same rules andregulations that apply to JBM Group owned equipment.

6.3.2 Risk Assessment Policy

Risk assessments can be conducted on any entity within JBM Group or any outside entity that has signed a *Third Party Agreement* with JBM Group, RAs can be conducted on any information system, toinclude applications, servers, and networks, and any process or procedure by which these systems areadministered and/or maintained.

The execution, development and implementation of remediation programs is the joint responsibility of IT and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable.
Employees are further expected to work with the IT Risk Assessment Team in the development of aremediation plan.

6.3.3 Policy Compliance

6.3.3.1 Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to,business tool reports, internal and external audits, and feedback to the policy owner.

6.3.3.2 Exceptions

Any exception to the policy must be approved by the Plant IT team in advance.

6.3.3.3 Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action based on JBM Group IT recommendation on case-to-case basis and actions will be taken by HR team.

6.3.4 Internet Usage Policy

6.3.4.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee’s current job responsibilities upon the request received from the respective department heads.

User Internet access requirements will be reviewed periodically by IT departments to ensure that continuing needs exist.

6.3.4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Any queries can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes.
- IT technical support downloading software upgrades and patches.
- Review of vendor web sites for product information.
- Reference regulatory or technical information.
- Research

6.3.4.3 Personal Usage

Using company computer resources to access the Internet for personal purposes, without approval from the user’s manager and the IT department, may be considered cause for disciplinary action up to and including termination which will be case to case dependent.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

6.3.5 Prohibited Usage

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race,sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise harmful or discredit materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personneldata with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling activities is also strictly prohibited:
- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.
- Any ordering (shopping) of items or services on the Internet.

- Playing of any games.
- Forwarding of chain letters.
- Participation in any on-line contest or promotion.
- Acceptance of promotional gifts.

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation and may ban the downloading of particular file types.

6.3.6 Software License

The company strongly supports strict adherence to software vendors' license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk.

6.3.7 Expectation of Privacy

6.3.7.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

6.3.7.2 Maintaining Corporate Image Representation

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

6.3.7.3 Company Materials

Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service.

Any posting of materials must be approved by the employee's manager and will be placed by an authorized individual.

6.3.8 Policy Compliance

Compliance Measurement

IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Corporate IT Team in advance.

Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
Additionally, the company may at its discretion seek legal remedies for damages incurred because of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the Internet via company network is approved, the potential Internet user is required to read the Internet usage Policy and sign an acknowledgment form. The signed acknowledgment form should be turned in and will be kept on file at the facility granting the access. For questions on the Internet usage Policy, contact the Information Technology (IT) Department.

6.4 Password Policy

The scope of this policy includes all personnel who have or are responsible for an account (or any formof access that supports or requires a password) on any system that resides at any JBM Group facility, has access to the JBM Group network, or stores any non-public JBM Group information.

6.4.1 Policy

6.4.1.1 Password Creation

6.4.1.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

6.4.1.1.2 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.

6.4.1.1.3 User accounts that have system-level privileges granted through group memberships or programs such as Sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

6.4.1.2 Password Change

6.4.1.2.1 Passwords should be changed every 90 days and not only when there is reason to believe a password has been compromised.

6.4.1.3 Password Protection

6.4.1.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as confidential JBM Group information.

6.4.1.3.2 Passwords must not be inserted into email messages, WhatsApp, SMS or other forms of electronic communication, nor revealed over the phone to anyone.

6.4.1.3.3 Passwords should not be stored by the users in file servers.

6.4.1.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

6.4.1.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

6.4.1.4 **Application Development**

Application developers must ensure that their programs contain the following security precautions:

6.4.1.4.1 Applications must support authentication of individual users, not groups.

6.4.1.4.2 Applications must not store passwords in clear text or in any easily reversible form.

6.4.1.4.3 Applications must not transmit passwords in clear text over the network.

6.4.1.4.4 Applications must provide for some sort of role management; such that one user can take over the functions of another without having to know the other's password.

6.4.1.5 Multi-Factor Authentication

6.4.1.5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

6.4.2 Password Construction Guidelines

Strong passwords are long; the more characters you have the stronger the password. We recommend a **minimum of eight characters in your password**. In addition, we highly encourage the use of passphrases,passwords made up of multiple words with at least one Capital letter, lower case, special character and numerals (Eg. P@ssw0rd1). Passphrases are both easy to remember and type yet meet the strength requirements.

6.4.2.1 Users must avoid using common or easily guessable passwords such as "password123," "admin123," or personal information (e.g., name, birthdate).

In addition, every work account should have a different, unique password. Whenever possible, alsoenable the use of multi-factor authentication.

7. Abbreviation

Sr. No	Term	Abbreviation
1	InfoSec	Information Security
2	IT	Information Technology
3	RA	Risk Assessment
4	CIO	Chief Information Officer
5	VPN	Virtual private network
6	USB	Universal Serial Bus
7	WWW	World Wide Web
8	PC	Personal computer