JBM GROUP

Cyber Security Policy Template

JBM GROUP	Document No.	
	Rev No.	
Title: Cyber Security Policy Template	Effective Date	
	Page	1 of 13

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 in serving the interests of the company and of our clients and customers in the course of 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 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within JBM Group may monitor equipment, systems and network traffic at any time, per *InfoSec's Audit Policy*.

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 connect to the internal network must comply with the *Minimum Access Policy*.

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 Postings by employees from JBM Group email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of JBM Group, unless posting is in the course of business duties.

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 the course of 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 is illegal 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 which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or 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.
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's, and the installation of any copyrighted software for which or the end user does not have an active license is strictly prohibited.
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. 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.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, Phishing mails, Ransomware, etc.).
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.
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.
8. Making fraudulent offers of products, items, or services originating from any JBM Group account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. 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.

11. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.

12. 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.

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

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

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

16. 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.

17. 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". Questions may be addressed to the IT Department

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).

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

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

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.

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

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.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

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, provided that it is done 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.

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 or any other material covered by JBM Group's Confidential Information policy when engaged in blogging.

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 JBM Group's *Non-Discrimination and Anti-Harassment* policy.

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 any and all risk associated with blogging.

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 Classification Policy
- Data Protection Standard
- Secured Access Policy
- Password Policy

1. DATA Classification Policy

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 to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

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 one of JBM Group's networks. Software applications running on JBM Group's networks may require access to one of the many internal database servers. In order 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.

2. DATA Protection Standard

Recommended processes to prevent virus problems:

- Always run the Corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- 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 by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with JBM Group's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan an external disk (Pen drive, mem card etc.,) from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- Run the anti-virus utility to ensure a clean machine, isolate the machine from network and take support from IT team, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Periodically check whether *Anti-Virus updates* are happening towards processes list for updates.

Disaster Recovery Plan Policy

Policy Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on Half yearly basis.

Removable Media Policy

JBM Group staff may only use JBM Group removable media in their work computers. JBM Group removable media may not be connected to or used in computers that are not owned or leased by the JBM Group without explicit permission of the JBM Group IT staff. 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, it must be encrypted with Bit locker in accordance with the JBM Group *Acceptable Encryption Policy*. 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.

3. Secured Access Policy

VPN Access

Approved JBM Group employees authorized may utilize the benefits of VPNs, which are a "user managed" 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 thirty minutes of inactivity. The user must then logon 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 with personal equipment, 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 and regulations that apply to JBM Group owned equipment, i.e., their machines must be configured to comply with necessary legal Antivirus and Operating System security updates.

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, to include applications, servers, and networks, and any process or procedure by which these systems are administered 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 a remediation plan.

Policy Compliance

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.

Exceptions

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

5.1 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action based on JBM Group IT recommendation.

Internet usage Policy

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. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days.

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

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. Questions 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 possible vendor web sites for product information;
- Reference regulatory or technical information.
- Research

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.

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

Prohibited Usage
Information stored in the wallet, or any consequential loss of personal property.

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 libelous 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 personnel data 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 are 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.

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.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

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.

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.

Review of Public Information

All publicly-writeable directories on Internet-connected computers will be reviewed and cleared. This process is necessary to prevent the anonymous exchange of information inconsistent with company business. Examples of unauthorized public information include pirated information, passwords, credit card numbers, and pornography.

Expectation of Privacy

1.1 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.

1.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

1.3 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".

1.4 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 the public relations department and will be placed by an authorized individual.

1.5 Creating Web Sites

All individuals and/or business units wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained through the IT Department. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the Corporate Communications Directors for initial approval to continue. All company pages are owned by, and are the ultimate responsibility of, the Corporate Communications Directors.

All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the IT department.

1.6 Periodic Reviews

Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

1.7 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

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 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 as a result 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.

4. Password Policy

The scope of this policy includes all personnel who have or are responsible for an account (or any form of 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.

Policy

4.1 Password Creation

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

4.1.2 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.

4.1.3 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.

4.2 Password Change

4.2.1 Passwords should be changed only when there is reason to believe a password has been compromised.

4.2.2 Password cracking or guessing may be performed on a periodic or random basis by the IT Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential JBM Group information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

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

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

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

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

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

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

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

4.5.4 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.

4.6 Multi-Factor Authentication

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

Password Construction Guidelines

Strong passwords are long; the more characters you have the stronger the password. We recommend a minimum of 8 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

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