Information Security Management System
Cyber Security Policy

Document no. JMBGRP/ISMS/Pol-GCS

Version no. v1.1

Document details

Classification	Internal	
Released date	10.04.2022	
Description	This document outlines the Cyber Security policy for JMBGRP to manage the risk of data theft, scams, and security breaches can have a detrimental impact on a JMBGRP's system, technology infrastructure, and reputation. It provides guideline to all stakeholders to deal with information shared through unsecured platform like internet.	
Custodian	Corporate IT dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT dept.	

Distribution list

Name
The policy applicability is irrespective to any designation and location; hence distribution is for all levels in all JMBGRP of companies.

Version History

Version no.	**Version date**	**Approved by**	**Comments**	**Signature**
0.1	01.04.2022	NA	Initial draft	NA
0.2	06.04.2022	NA	Revised draft - new points were added 3.1.5, 3.1.6, 3.1.7 and 3.1.8 based on 1st level policy discussion	NA
1.0	10.04.2022	Manish Jaiswal (Group CTO)	Restructuring document as per approved template and points are revised 1st release	
1.1	18.08.2023	Manish Jaiswal (Group CTO)	Restructuring document as per approved template and points are revised 1st release	
1.2	16.10.2024	Manish Jaiswal (Group CTO)	Reviewed & no change	

Contents

1.0 Purpose

JMBGRP cyber security policy outlines guidelines and provisions for preserving the security of group's data and technology infrastructure.

The risk of data theft, scams, and security breaches can have a detrimental impact on a JMBGRP's system, technology infrastructure, and reputation. As a result, JMBGRP has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

This policy is supported by the thoroughly defined information security policies' set which ensures of every technical aspects of the applicable controls are identified, controlled, and managed.

2.0 Scope

This policy applies to all JMBGRP employees, contractors, volunteers, and anyone who has permanent or temporary access to systems and hardware.

3.0 Policy Statement

3.1 Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)
- Privacy information of individuals including client and all types of employees

It is mandatory for all (employees and contract employees, vendors) protect this data. Through this policy, JMBGRP providing of instructions to be followed how to avoid security breaches.

3.1.1 Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to group's data. It is advised to employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.

- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks (VPN) only.

JMBGRP also advise employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new hires receive company-issued equipment they will receive instructions as a part of information security induction trainings or as and when they receive the equipment.

They should follow instructions to protect their devices and refer to IT cell if they have any questions.

3.1.2 Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, JMBGRP instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-away (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email, they received is safe, they can refer to IT cell.

All emails are observed through additional email security which ensures email scan (incoming/outgoing) are verified for the security threats (e.g. spam, fishing and spear fishing, business email compromise etc.)

3.1.3 Manage passwords properly

Password leaks are serious since it has potential to compromise entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this purpose, we advice employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

3.1.4 Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask IT cell for help.
- Share confidential data over the company network/ system and not over public Wi- Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts
- Employees shall not transfer personal identifiable information or the practice's business information via the internet without prior approval of the Security Officer.
- Before transmitting individually identifiable health information, the user will comply with group's Privacy Policy to ensure legal authority for the disclosure exists.
- The Data Privacy Officer is responsible for ensuring Business Associate Agreements are in place to protect the security and confidentiality of information transmitted via the internet when necessary.

J. M Baxi Group IT Cell need to know about scams, breaches and malware so they can better protect infrastructure. For this reason, we advise employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to specialists. IT Cell must investigate promptly, resolve the issue and send a companywide alert when necessary.

Security Specialists are responsible for advising employees on how to detect scam emails. We encourage employees to reach out to them with any questions or concerns.

We follow simulation method to train company email users.

3.1.5 Access control

3.1.5.1 Internet access control

All employees and other users must strictly observe the following rules when using the internet:

- Employees should access or use the internet for official business purpose and circumvent usage for personal commercial gain.
- Employees are strictly forbidden from accessing pornographic or other offensive websites (including, but not limited to, sexist, racist, discriminatory, hate, or other sites that would offend a reasonable person in the same or similar circumstances). If the user has any doubt whether access to a specific site is proper, he or she should seek approval from the Security Officer.

3.1.5.2 System, application, and privilege access control

- Users should use own user's ID, password and refrain from using other identification to access the internet.
- Users attempting to establish a connection with this office's computer system via the internet must authenticate themselves at a firewall using VPN before gaining access to its internal network.
- Employees should avoid establishing access to modems, internet, or other external network connections that could allow unauthorized users to access systems or information without the prior approval of the Security Officer.
- Employees shall refrain from establishing or using new or existing internet connections to establish new communications channels without the prior approval of the IT Cell.
- Risk assessment shall be done for defining level of controls to the information assets

- Privilege access management is carefully handled to secure information assets from being compromised.
- For each application or module, the business should nominate a System Owner who should undertake a risk assessment, specify access requirements and monitor their overall implementation.
- Applications will be accessed via mechanisms that conform to Group standards and are consistent with the risk assessment.
- All access permissions will be granted in accordance with an approved process.
- Access to financial and sensitive data as identified in the Information Classification and Handling Policy should follow the principle of 'segregation of duties'.
- The System Owner shall conduct reviews of access permissions, periodically,
- System owner shall ensure the control transmission of data internal as well as external networks.

3.1.6 Cyber security incident response

IT and cybersecurity professionals design proactive and reactive measures which are intended to circumvent the incidents as it hits the perimeters of the company's IT infrastructure or respond to the security incidents happened despite of all possible precautionary measures taken, respectively.

IT and cybersecurity professionals should immediately respond to a serious cyber security incident, such as a data breach, data leak, ransomware attack, or loss of sensitive information.

An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered.

The incident response phases are:

- **Preparation**

  Employees shall be trained with respect to their incident response roles and responsibilities in the event of data breach,

  - Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.

  - Ensure that all aspects of incident response plan (training, execution, hardware, and software resources, etc.) are approved and funded in advance

- Response plan should be well documented, thoroughly explaining everyone's roles and responsibilities. Plan must be tested for assuring that employees shall perform as trained.

- **Identification**

  To determine whether there is a breach and its severity in terms of extent of breach and damage to JMBGRP. Also, incident shall be identified for its origination and best possible remediation possible with current capabilities.

- **Containment**

  - When a breach is first discovered, contain the breach so it doesn't spread and cause further damage to business.
  - Disconnect affected devices from the network
  - Have short-term and long-term containment strategies ready.
  - Use redundant system back-up to help restore business operations.
  - Patch your systems, review your remote access protocols (requiring mandatory multi-factor authentication),
  - change all user and administrative access credentials and harden all passwords.

- **Eradication**

  - Identify and eliminate the root cause of the breach.
  - all malwares should be securely removed, systems should again be hardened and patched, and updates should be applied.
  - In case this activity should be performed by third party, engagement with the third party should be thorough.

- **Recovery**

  - restoring and returning affected systems and devices back into your business environment.
  - get systems and business operations up and running again without the fear of another breach.

- **Lessons Learned**

  - IT and cybersecurity professionals should maintain system log and activity log and

secure for learnings

- On investigation completion, after-action meeting will be conducted with all Incident Response Team members and discuss the learnings from the data breach. Determine the effectiveness of the response plan, and where there were some security loopholes. Lessons learned from both mock and real events shall help strengthen your systems against the future attacks.

3.1.7 Employee Awareness Trainings

Employees should be trained for ensuring security awareness and training controls that protect the confidentiality, integrity, and availability of the JMBGRP's Information assets, Employees trainings may be of;

- General information security awareness training
- Security awareness – insider threats training
- Role-based security trainings

Trainings effectiveness is verified time to time to encourage upgradation needs in training programms or schemes.

3.1.8 Third-party security

JMBGRP to ensure the security requirements for protecting confidentiality, integrity and availability of business-critical information are satisfied and maintained when a business process or processes are partially or completely entrusted to a vendor or outsourced.

- Risk assessment shall be performed prior granting a logical or physical access to the external party.
- Strict access control at all levels for ensuring the information would be available on need-to-know basis and to fulfil the contractual obligations to the third party.
- Protection of the privacy information shall be ensured by third party and same would be assured by well-defined contractual clauses inclusive of audit, compliance, indemnifications and penalties.
- Sign agreements which shall address clauses related duration/ non-disclosure/ confidentiality/exchange of information and software in physical and electronic modalities/service delivery and commitment/levels of physical and logical access and their duration thereof. The agreement shall also have relevant clauses related to creation/storage/transmission/destruction of information assets created in soft/hard form on behalf of JMBGRP or for JMBGRP.
- Monitoring and review of third-party services shall be carried out to ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly.

3.2 Additional measures

To reduce the likelihood of security breaches, we also instruct employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to [HR/ IT Department].
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on their company equipment.
- Avoid accessing suspicious websites.

JMBGRP also expect employees to comply with group's social media and internet usage policy.

Security Specialists/ Network Administrators should:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

JMBGRP will have all necessary physical and digital shields to protect information.

3.3 Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing JMBGRP's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

JMBGRP encourage them to seek advice from our IT Cell.

3.4 Disciplinary Action

J. M Baxi Group expect all employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: HR may issue a verbal warning and train the employee on security.
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): JMBGRP shall invoke more severe disciplinary action up to and including termination.
- All incidents shall be examined thoroughly on a case-by-case basis.

Additionally, employees who are observed to disregard security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

3.5 Take security seriously

Everyone, of JMBGRP's customers and partners to employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect JMBGRP systems and databases. JMBGRP can all contribute to this by being vigilant and keeping cyber security top of mind.