CYBER SECURITY POLICY

Cyber Security Policy for Jaiprakash Power Ventures Limited & its Subsidiaries

Cyber security refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. Dealing with the security of **Cyberspace**, the virtual environment where people and software interact over a complex web of computer networks, Cyber Security is on the path towards gaining increasing prominence as we move towards a technology driven future.

The core functionality of cyber security involves protecting information and systems from major cyber threats. These cyber threats take many forms (e.g., application attacks, malware, ransomware, phishing, exploit kits).

Some of the common threats are outlined below in more detail.

Cyberterrorism is the disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes the form of attacks on networks, computer systems and telecommunication infrastructures.

Cyberwarfare involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption. In the U.S. and many other nations, cyber warfare has been acknowledged as the fifth domain of warfare (following land, sea, air and space). Cyber warfare attacks are primarily executed by hackers who are well-trained in exploiting the intricacies of computer networks, and operate under the auspices and support of nation-states. Rather than "shutting down" a target's key networks, a cyber-warfare attack may intrude into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.

Cyberespionage is the practice of using information technology to obtain secret information without permission from its owners or holders. Cyber espionage is most often used to gain strategic, economic, political or military advantage, and is conducted using cracking techniques and malware.

Cyber Security policy broadly covers following three areas as :

1. **Physical security:** It mandates what protection should be wielded to safeguard the physical asset for both employees and management, applies to the prevail facilities including doors, entry point, surveillance, alarm, etc.
2. **Personnel management:** Tell employees how to conduct or operate day to day business activities in a secure manner, for instance, password management, confidential information security, etc., applies to individual employees.
3. **Hardware and software:** It directs the administrator what type of technology to use and what and how network control should be configured and applies to system and network administrators.

Hardware Cyber Security Concerns:

Most equipment and technology for setting up Cyber Security infrastructure in India are currently procured from global sources. These systems are vulnerable to cyber threats just like any other connected system.

There are various types of hardware attacks that may pertain to various devices or systems like:

- Network systems
- Authentication tokens and systems
- Surveillance systems
- Control systems
- Communication infrastructure devices

Policy brief & Purpose:

JaiprakashPower Ventures Limited (JPVL) Cyber Security Policy outlines guidelines and provisions for preserving the security of its Data and Technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

We have adopted a layered security approach in the organization. There are security devices and software in the entire IT infrastructure including the network by implementing appropriate hardening measures. Servers, Local Area Network (LAN) and Wide Area Network (WAN) infrastructure is secured by installing appropriate perimeter security devices such as **Firewalls, Server load balancer, Application proxy, Intrusion Prevention System, Anti-spam, Anti-virus system, SSL-VPN and DMZ zone** and methods to log and monitor the events to detect network scanning, probing and Reconnaissance attempts on the IT infrastructure.

Scope:

This policy applies to all our employees, contractors, volunteers, hardware consultants, service provider or anyone who has permanent or temporary access to company assets such as computer networks data information or any information that is perceived to be valuable to the business.

Policy Elements:

- Confidential Data
- Protect personal and company devices
- Keep Emails Safe
- Manage passwords properly
- Transfer data securely
- Data Retention
- Additional measures
- Remote employees

Confidential Data :

Confidential data is secret and valuable. Common examples are:

- Software &Applications
- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we shall give our employees instructions on how to avoid security breaches.

Protect personal and company devices:

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep 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 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 only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. They should follow instructions to protect their devices and refer to our IT Support / Information Security Team if they have any questions.

Keep Emails Safe:

Emails often host scams and malicious software (e.g. worms/ransomeware). To avoid virus infection or data theft, we 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, Account is locked")
- Be suspicious of click bait 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-aways (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 our Information Security Team / Mailing Team / IT Support team.

Manage passwords properly:

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we have group policy and advise our 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.

Transfer data securely:

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. Software & Applications, 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 our IT Support team / Information Security Team 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

Our IT Support / Information Security Team need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our Information Security Team must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our Information Security team is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Data Retention:

- Archiving: Organizational records, including sensitive information records (especially mails) which are not being used for active organization business, may be archived until retention requirements have been met.
- Departments determine the criteria for inactive record status in their areas, based on need for the records and available storage space and public records law.
- Storage areas for inactive records must be physically secure and environmentally controlled, to protect the records from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.
- When appropriate, only primary records should be archived. The contents of true “Shadow” records should be destroyed after it has been determined that they contain

only duplicates of records maintained elsewhere, and do not contain any original materials.

- Off-site storage facilities or locations for sensitive records must be approved by Administration Department.

AdditionalMeasures:

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

- Turn off their screens and lock their devices when leaving their desks. We have applied group policy in server to lock screen after 3 minutes of inactivity.
- 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

Our IT Support team / Information Security team:

- Install firewalls, antivirus & 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 these policies provisions as other employees do.

- Configuration of security devices is checked at the time of installation as well as at the time of significant changes for the needed functionalities and security features.
- Dedicated backup management team to take care critical servers & services data backup and restore.
- We have implemented Information Security Management System as per ISO 27001 standard to prevent cyber security incidents.
- We carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with business impact assessment and criticality of business functions.
- Nominated **Chief Information Security Officer (CISO)** to co-ordinate the security related issues/implementation within the organization.
- Dedicated Information Security Team is working under CISO.

Information Security Team broadly provide following services:

(a) Response to cyber security incidents

(b) Prediction and prevention of cyber security incidents

(c) Analysis and Forensics of cyber security incidents

(d) Information Security Assurance

(e) Awareness and technology exposition in the area of cyber security

(f) Training/Upgrade of technical know-how for the end users

Prevention and Precautionary Measures to avoid cyber attack

- Develop and implement a business continuity strategy and contingency plan
- Nomination of Chief Information Security Officer
- Information Security Policy & implementation of best practices
- Business Continuity Plan (BCP)

- Security incident management processes
- Disaster Recovery Plan (DRP)
- Security of Information infrastructure and network
- Network traffic scanning
- Isolation of critical networks
- Implementation of Security guidelines issued by concerned authorities
- Background checks
- Audit & Assurance
- Security training & awareness
- Sharing of information pertaining to incidents
- Penetration testing (both announced and unannounced)
- Vulnerability assessment
- Application security testing
- Web security testing
- Keep your operating systems up to date with critical security updates and patches.
- Read Privacy policy carefully when you submit the data through internet.
- Disable remote Desktop Connections, employ least-privileged accounts.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Use antivirus software and firewalls –keep them up to date
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Restrict user's abilities (permissions) to install and run unwanted software applications.

- Do not Open share (Everyone Full Rights) on systems.
- Lock down mapped network drives by securing them with a password and access control restrictions.
- Disable auto-run on systems (through antivirus / windows patch)
- Create rule in desktop antivirus to stop Executable files running from CD/DVD, USB & Network drives.
- Block USB access on desktop.
- Have a pop-up blocker running on your web browser.
- Install Good Security / IPS/ Content filter / Anti Spam / Firewall Appliance at Gateway level.
- In case of suspected virus attack, Isolate the infected computer before the virus / ransomeware can attack network drives to which it has access and perform full scan, update, remove virus from it. Restore damaged files from a known good backup.

Remote Employees:

Remote employees must follow this policy's instructions too. Since they shall be accessing our company'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. We encourage them to seek advice from our IT Support team / Information Security Team.

Disciplinary Action:

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We shall invoke more severe disciplinary action up to and including termination. We shall examine each incident on a case-by-case basis.
- Additionally, employees who are observed to disregard our security instructions shall face progressive discipline, even if their behavior hasn't resulted in a security breach.

Steps to Cyber Security:

1. **Network Security** Protect your networks against external and internal attack. Manage the network primer. Filter out unauthorised access and malicious contents. Monitor and test security controls

2. **Malware Protection** Produce relevant policy and establish anti-malware defenses that are applicable and relevant to all business areas. Scan for malware across the Organisation.

3. **Monitoring** Establish a monitoring strategy and produce supporting policies. Continuously monitor all system and networks. Analyze logs for unusual activity that could indicate an attack. . Monitoring user activity allows you to detect unauthorized behavior and verify user actions are not violating security policy.

4. **Incident Management** Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

5. **User Education and Awareness** Produce user policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

6. **Home and Mobile Working** Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline to all devices. Protect data both in transit and at rest.

7**. Secure Configuration** Apply security patches and ensure that the secure configuration of all systems is maintained. Create a system inventory & define a base line build for all devices. To keep our network protected, make sure software and hardware security is up to date with the latest and greatest.

8. **Removable Media Controls**produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before imported on the corporate system.

9. **Managing User Privileges** Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

10.Information Risk ManagementRegime Establish and effective governance structure and determine your risk appetite. Maintain Board's engagement with cyber risk. Produce supporting information risk management policies.

11.Outline Clear Use Policies for New Employees and 3rd Parties Clearly outline the requirements and expectations the company has in regards to IT security when you first hire them. Make sure employment contracts and SLAs have sections that clearly define these security requirements.

12. Beware of Social Engineering Social engineering tactics have been used successfully for decades to gain login information and access to encrypted files. Attempts may come from phone, email or other communications with our users. The best defense is to…

13.Educate and Train Your Users Training should include how to: recognize a phishing email, create and maintain strong passwords, avoid dangerous applications, ensure valuable information is not taken out of the company in addition to other relevant user security risks. Training people on proper cyber security hygiene is critically important.

14.Back Up Data It is crucial for organization to have a full working back up of all of data not only from a basic security hygiene prospective, but also to combat emerging attacks.

15. Stop Data Losst is extremely important to control access, monitor vendors and contractors as well as employees, and know what your users are doing with company data to reduce data leakage.

Related Policies and Processes

The above Policy outlines the cyber security Policy for **Jaiprakash Associates Limited& Its subsidiaries** however,**following five additional policies**extend its base and strengthen the controls further:

- ✓ **Acceptable Use policy**
- ✓ **E-mail Policy**
- ✓ **Password Policy**
- ✓ **Internet Use, Access & Browsing Policy**
- ✓ **Communications and Operations Management Policy**:

Policy Compliance

Compliance Measurement

The Information Security Team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to thisPolicy must be approved by the Chief Information Security Officer (CISO) in advance and then by Director in Charge with subsequent approval of the Managing Director/ Chairman.

Non-Compliance

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