



## Cyber Security and Data Privacy Policy

### Objective

All Employees and personnel, more particularly detailed hereinbelow, of Balajee Infratech & Constructions Private Limited ("BALAJEE GROUP"), and unless repugnant to the context or meaning thereof, its subsidiaries, associates, affiliates, executors, successors in interest and assigns (hereinafter collectively with BALAJEE GROUP referred to as the "BALAJEE Group"), recognize the importance of cyber security and data privacy in ensuring growth and information security across the organisation. Well protected Information systems and data resources of BALAJEE Group are critical to business operation continuity and sustainable growth.

The objective of this Cyber Security and Data Privacy Policy (hereinafter referred to as "Cyber Security and Data Privacy Policy" or "Policy") is to set standards and/or framework for the usage and protection of confidential data related to the organization. This Policy intends to communicate the organization's commitment in terms of protecting the Data of BALAJEE Group, its clients, its employees and any other third party temporarily or permanently affiliated with the BALAJEE Group. It is evidence of the BALAJEE Group's commitment to data protection principles.

### Scope & Applicability

This document shall be valid and binding on all the employees and or any of the part time/ full time staff of BALAJEE Group.

BALAJEE Group takes reasonable measures and precautions to maintain privacy and confidentiality of its internal firm data, confidential client data, personal data collected from employees and other data collected from third parties. It has put in place Reasonable Security Practices and Procedures for protection of personal sensitive and confidential data.

### Definitions

1. "Data" means a representation of Information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

2. **"Information"** includes Data, message, text, images, sound, voice, codes, computer programmes, software and data bases or microfilm or computer-generated micro fiche.
3. **"Password"** means a secret word or phrase or code or passphrase or secret key, or encryption or decryption key that one uses to get admittance or access to Information.
4. **"Personal Information"** means any Information that relates to a natural information which, either directly or indirectly, in combination with other Information available or likely to be available with a body corporate is capable of identifying such person.
5. **"Body Corporate"** means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.
6. **"Reasonable Security Practices and Procedures"** means security practices and procedures designed to protect such Information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such Reasonable Security Practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.
7. **"Sensitive Personal Data or Information"** means such Personal Information which consists of Information relating to:
  - a. Password;
  - b. Financial information such as Bank account or credit card or debit card or other payment instrument details;
  - c. Physical, physiological and mental health condition;
  - d. Sexual orientation
  - e. Medical records and history;
  - f. Biometric information;
  - g. Any detail relating to the above clauses as provided to Body Corporate for providing service; and
  - h. Any of the information received under above clauses by Body Corporate for processing, stored or processed under lawful contract or otherwise;Provided that, any information that is freely available or accessible un public domain or furnished under the Right of Information Act, 2005 or any other law for the time being in force shall not be regarded as Sensitive Personal Data or Information.

## Policy Definition

The Cyber Security and Data Privacy Policy of the BALAJEE Group is set on the lines of the law to be compliant to standardize the use, monitoring, and management of Data. The main goal is to protect and secure all Data consumed, managed, and stored by the BALAJEE Group.

## General Policy Guidelines

1. BALAJEE Group supports the right to privacy, including the rights of individuals to control the dissemination and use of Personal Information that describes them, their personal choices or life experiences.
2. BALAJEE Group supports the laws and regulations that seek to protect the privacy rights of such individuals.
3. BALAJEE Group seeks consent from individuals for obtaining Personal Information and the individual agrees to share the same in writing.



4. BALAJEE Group shall take reasonable efforts to make sure all Information maintained is accurate, timely, relevant and complete.
5. BALAJEE Group shall take reasonable efforts to make sure all Information is used and/or disseminated only as intended.
6. Management of BALAJEE Group is responsible for establishing appropriate controls to ensure that private information is disclosed only to those who have a legitimate requirement for such access.
7. Sensitive Personal Data or Information shall not be retained for a period longer than required.
8. All entities granted access to the Information or Data shall sign a Non-Disclosure Agreement with BALAJEE Group.
9. All copies of Data including those on backup tapes, hard disks and such which are no longer needed must be irreversibly destroyed.
10. BALAJEE Group shall not be responsible for the authenticity of the Personal Information or Sensitive Personal Data or Information supplied by the provider of Information.
11. BALAJEE Group will take adequate measures to ensure Data protection and privacy.
12. When no longer required, all copies of Data including but not limited to those on backup tapes, hard-drives and/or any form of cloud storage must be irreversibly destroyed. Furthermore, a record mentioning the reason for destruction must be prepared and supplied to the Owner of said Information.

## **Policy Elements**

### **Confidential Data and Information**

Confidential Data and Information means any Data, Information or knowledge disclosed by BALAJEE Group or its Management, affiliates or employees and not generally known to the public, including but not limited to:

1. The BALAJEE Group's business or operational plans or activities, existing or contemplated markets, advertising initiatives, methods of operation, products, or services.
2. The BALAJEE Group's Data on its suppliers, logistics or employees.
3. The BALAJEE Group's customer or supplier lists, cost of goods or services, profits and losses, budgeting, past or future sales, or financial information.
4. The BALAJEE Group's schematics, designs, software source or object code, compressed or uncompressed binaries, inventions, patents or patent applications or illustrations.
5. The BALAJEE Group's existing or contemplated designs, models or platforms, formulas, notes, or analytical data.
6. The BALAJEE Group's management, board of directors, affiliates, suppliers, customers, employees, or third-party contractors.
7. The BALAJEE Group's history, entity structure, accounts, or goodwill; the Company's copyrights, trademarks, trade secrets, patents, trade names, moral rights, or any other tangible or intangible rights, whether registered or unregistered.
8. The BALAJEE Group's technical systems, processes, methods, algorithms, computational schemas, know-how, or trade secrets.
9. The BALAJEE Group's employees, salaries, job related functions, duties or responsibilities.
10. The BALAJEE Group's written, verbal or electronic communications.



11. Any Personal Information of an employee of BALAJEE Group which can be used to identify, contact or locate the person to whom such Information pertains, which includes but is not limited to the name, address, email, biometric information.
12. Employee's Health Information relating to past/present/future, physical or mental, recorded by BALAJEE Group.
13. Any confidential or proprietary data relating to a client's business and any other Information subject to professional secrecy, confidentiality and/or proprietary by a client which may include but is not limited to business practices, marketing plans, mergers and acquisitions data, financial information, names of clients in certain cases and the description of the work being performed.
14. Any Information that if disclosed, whether true or untrue, could harm the goodwill or reputation of the BALAJEE Group or the management, board of directors, affiliates, suppliers, customers, employees, third-party contractors, methods of operation, products, or services.

### **Protect Company Devices**

When employees use their digital devices to access company emails or accounts, they introduce security risk to the Data of BALAJEE Group. The employees are advised to keep both their personal and company-issued computer, tablet, and cell phone secure. To ensure this, the following measures can be taken:

1. All devices must be Password protected
2. Antivirus software must be timely updated.
3. Devices should not be exposed or left unattended.
4. Install security updates of browsers and systems monthly or as soon as updates are available.
5. Log into company accounts and systems through secure and private networks (office & home network) only.
6. Employees should not access internal systems and accounts from other people's devices
7. Employees must not share Company devices with persons other than employees of BALAJEE Group.

### **Keep Emails Safe**

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or Data theft, Employees are instructed to ensure the following:

1. Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
2. Be suspicious of clickbait titles (e.g. offering prizes, advice.)
3. Check email and names of people they received a message from to ensure they are legitimate.
4. Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
5. If an employee isn't sure that an email, they received is safe, they must refer to our ITS Department

### **Manage Passwords Properly**

Password leaks are dangerous since they can compromise the entire infrastructure of BALAJEE Group. Not only should Passwords be secure but also be kept confidential. For this reason, Employees are advised to:



1. 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.)
2. 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.
3. Exchange credentials only when necessary.
4. Change their Passwords every two months.
5. Perform antivirus security sweeps on their devices on a regular basis.

## **Transfer Data Securely**

Transferring Data introduces security risk. Employees must:

1. Avoid transferring Sensitive Personal Data or Information (e.g. customer information, employee records) to other devices or accounts unless necessary. When mass transfer of such Data is needed, employees are requested to take advice ITS Dept.
2. Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
3. Ensure that the recipients of the Data are properly authorized people or organizations and have adequate security policies.
4. Report scams, privacy breaches and hacking attempts, [IT Specialists/ Network Engineers] 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 Network Engineers must investigate promptly, resolve the issues, and send a companywide alert when necessary.
5. The ITS Department is responsible for advising employees on how to detect scam emails. Employees are encouraged to reach out to them with any questions or concerns.

## **Data Back-up, Retention and Recovery**

Data protection is one of the key areas of the Cyber Security and Data Privacy Policy. At BALAJEE Group, all servers and computers have been secured through robust backup and recovery mechanisms. The details of the SOP are defined in the 'ITS Manual for Data Backup and Restore'. To further reduce the Data loss, employees are advised to:

1. Follow suitable and concise naming conventions to all files created by them.
2. Avoid including special characters except hyphen '-' and space ' ' in file names.
3. Follow defined directory structure to store relevant files.
4. Do not keep multiple copies of the same file and if necessary, maintain version number

## **Work From Home Measures**

Work From Home facility shall be granted to the employees on exceptional cases and in such event the employee shall strictly adhere to the terms and conditions of this policy. The employees are also required to:

1. Connect to office VPN through secured private network only.
2. Not use any public / free internet networks.
3. Not enable hotspot / Bluetooth applications through devices connected to office VPN.



## **Additional measures**

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

1. Turn off their screens and lock their devices before leaving their desks.
2. Report stolen or damaged equipment as soon as possible to [HR/ ITS Department].
3. Change all account Passwords at once when a device is stolen.
4. Report a perceived threat or possible security weakness in company systems.
5. Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
6. Avoid accessing suspicious websites.
7. To comply with our social media and internet usage policy.

Hardware Specialists/ Network Administrators should:

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

## **Data Integrity**

BALAJEE Group will take reasonable steps to ensure that the process Data is accurate, reliable and current by reviewing the Information as follows:

1. Updating existing Information.
2. Adding new Information when received.
3. Ensuring non-duplication of Information.
4. Making use of correct Data elements
5. Including sufficient identifiable Information
6. Avoiding the use of inaccurate identifies (For example, Employee ID number)

## **Distribution of Information to Third Parties:**

BALAJEE Group may be required to share confidential information with governmental agencies or other companies assisting in fraud prevention or investigation. BALAJEE Group may do so:

1. When permitted or required by law
2. To protect or prevent potential fraud or unauthorised transactions
3. Investigation fraud which has already taken place.

This Information will not be provided for marketing purposes.

## **Onward Transfer Procedures:**

1. BALAJEE Group will not provide to a third party, Data without contractually committing that entity to appropriate protection of that Data.
2. When contracting with a new third party, BALAJEE Group will conduct due diligence on the new third party before transmission of Data.



## **Maintaining an Updated List of Third Parties:**

BALAJEE Group will maintain a list of third Parties with which contracts requiring compliance with BALAJEE Group were implemented. The list will include name of the company, list of effective dates and contract number.

BALAJEE Group will provide Information on a 'Need-to Know Basis', only disseminating the Information required to compile.

## **General Security Procedures**

Any relevant Data present in any form with BALAJEE Group:

1. When and if involved in any open investigation, audit or litigation shall not be destroyed or disposed of.
2. If so required, destroyed/disposed-off in a manner that cannot be recovered or reconstructed.

## **Disciplinary Action**

All employees are expected to adhere to this Policy and those who cause security breaches may face disciplinary action:

1. First-time, unintentional, small-scale security breach: A verbal warning shall be issued and training will be provided to the employee on security breaches.
2. On Intentional, repeated, or large-scale breaches (which cause severe financial or other damage): A severe disciplinary action will be invoked, including termination of employment.
3. Each incident will be examined on a case-by-case basis.
4. Progressive disciplinary action will be taken against employees who disregard the security instructions.

If BALAJEE Group gets notified or becomes aware of any inappropriate disclosure of Sensitive Personal Data or Information by third parties including but not limited to vendors, suppliers, contractors or sub-contractors, the following measures will be taken:

- a. Document the event and circumstances surrounding the event.
- b. Stop the practice of disclosure of the Sensitive Personal Data or Information
- c. Forward the report to the appropriate council
- d. Take steps to mitigate any negative impact that may result from the inappropriate disclosure
- e. Terminate the contract with the offending party



## Responsibility

1. Information Technology Services (ITS) department plays a vital role in implementing this Policy and ensuring adherence to this Policy across the organization.
2. IT department, i.e. the IT Manager and/or chosen representative from the IT department, shall devise a comprehensive inventory cataloguing the storage locations of sensitive company Data.
3. The IT Manager should constantly be vigilant in maintaining IT security and controls similar to the adoption of Information security frameworks.
4. Manager/s and/or Business Head/s of the organization are strictly responsible for adhering to and ensuring the culture of Data confidentiality with respective teams.

| Date     | W. E. F. | Prepared By                                                                                            | Certified By | Approved By                                                                                               |
|----------|----------|--------------------------------------------------------------------------------------------------------|--------------|-----------------------------------------------------------------------------------------------------------|
| 12/11/24 | 12/11/24 | <br>Sr. Manager – ITS | —            | <br>Director – Finance |