# LiveBird Technologies Pvt Ltd.

# Information Security Policy

## 1. Purpose

This document delineates the guidelines and mechanisms by which LiveBird Technologies Pvt Ltd intends to protect the confidentiality, integrity, and availability of its information assets. These assets encompass but are not limited to software code, client data, company operational and financial data, intellectual property, employee information, and any other data crucial for the company's operations and reputation.

## 2. Scope

This policy is universally applicable within LiveBird Technologies Pvt Ltd and extends to all employees, contractors, vendors, and partners who access, manipulate, or manage company data in any format or platform. It covers all technological resources, including but not limited to computer systems, mobile devices, network equipment, software applications, and data storage facilities, whether physically on-site or hosted in cloud environments.

## 3. Policy Statement

LiveBird Technologies Pvt Ltd unequivocally commits to safeguarding its information assets from unauthorized access or compromise. The company will deploy a blend of physical, technical, and administrative security controls, adhering to industry best practices and regulatory requirements, to uphold the security triad: confidentiality, integrity, and availability of data.

## 4. Roles and Responsibilities

- Executive Management: Endorses and supports the ISP, ensuring it aligns with business strategy and legal obligations.
- Information Security Officer (ISO): Leads the development, implementation, and maintenance of the ISP, coordinating security initiatives and reporting on security posture to the executive management.
- IT Department: Implements technical security controls, manages IT infrastructure, and ensures system and data security through appropriate technologies and procedures.
- Human Resources (HR): Manages employee orientation and ongoing training on security policies, conducts background checks, and oversees the exit process to ensure the return of company assets and the revocation of access rights.
- Employees and Contractors: Must adhere to all aspects of the ISP, report security incidents, and ensure they do not knowingly compromise company information.

## 5. Asset Management

- Asset Inventory: Maintain a comprehensive inventory of all information assets, including their locations, custodians, and classification levels.
- Classification and Handling: Classify information assets based on sensitivity and criticality, implementing handling procedures that include labeling, storage, transmission, and destruction methods appropriate to the classification level.

## 6. Human Resources Security

- Pre-employment Checks: Conduct thorough background checks proportional to the job role's data access level.
- Security Training and Awareness: Provide all new hires with security training as part of their induction process, with mandatory annual refreshers for all staff. Specialized training will be provided based on specific job roles and access privileges.
- Disciplinary Process: Establish a clear process for addressing security breaches, which may include warnings, suspension, termination, and legal action, depending on the severity of the incident.

## 7. Physical and Environmental Security

- Secure Areas: Implement physical access controls to protect facilities and data centers, using mechanisms such as key cards, biometric scanners, and surveillance systems.
- Environmental Controls: Protect equipment from environmental threats and hazards with fire suppression systems, HVAC systems, and power supply backups.

## 8. Communications and Operations Management

- Operational Procedures and Responsibilities: Document and maintain standard operating procedures for IT and data handling tasks, ensuring a clear understanding of responsibilities and proper execution of tasks.
- Data Backup and Recovery: Regularly backup critical data, storing backups in a secure offsite location, and periodically test the restoration process to ensure data integrity and availability.

## 9. Access Control

- User Access Management: Implement strict procedures for granting, modifying, and revoking access to systems and data, based on the principle of least privilege and job requirements.
- User Responsibility: Establish clear guidelines for secure password management and the secure use of authentication tokens and devices.

## 10. Information Systems Acquisition, Development, and Maintenance

- Security Requirements: Integrate security considerations into the lifecycle of information systems, from the planning phase through development, deployment, maintenance, and decommissioning.
- Protection from Malware: Deploy and maintain anti-malware solutions across all endpoints and network entry points, regularly updating definitions and software.

## 11. Information Security Incident Management

- Incident Response and Management: Develop and maintain an incident response plan that includes incident detection, reporting mechanisms, response procedures, and recovery plans. Conduct regular drills to ensure preparedness.
- Learning from Incidents: Analyze and document security incidents to prevent recurrence, using findings to strengthen security measures and response strategies.

## 12. Compliance

- Legal and Regulatory Compliance: Regularly review and update security policies to comply with applicable laws, regulations, and industry standards, including data protection laws, intellectual property rights, and contractual obligations.

## 13. Policy Review and Evaluation

This policy will be reviewed at least annually or in response to significant changes in the business, technology, or the threat landscape, to ensure its relevance, effectiveness, and alignment with business objectives and regulatory requirements.

## 14. Acknowledgment

All LiveBird Technologies Pvt Ltd personnel must sign an acknowledgment form indicating they have read, understood, and agreed to comply with this Information Security Policy. This acknowledgment will be stored in each individual's personnel file.