# Information Security Policy

## 1. Purpose

The purpose of the Goodbaby International Group Information Security Policy is to define the overall approach to information security across the Goodbaby International group and its subsidiaries. This policy supports:

- The detection and prevention of information security breaches such as misuse of networks, data, applications and computer systems
- The preservation of the company's reputation, including compliance with ethical and legal responsibilities
- The respect of customer rights with regards to the classification, storage and processing of personal data

## 2. Audience

The intended audience of this policy is all Goodbaby International employees.

## 3. Information Security Objectives

Goodbaby International Information Security has the following objectives. In these objectives the term data is used to refer also to the systems, applications and networks that store, process and transmit the data, as well as any information on these systems.

• **Confidentiality**: To ensure only authorized users and processes are able to access or modify data

• **Integrity**: To ensure data is maintained in a correct state and that nobody is able to improperly modify it, either accidentally or maliciously

• **Availability**: To ensure authorized users are able to access the data they need, whenever they need to access it.

## 4. Information Security Principles

The Goodbaby International information security program is underpinned by six core principles. These principles will be used to guide any decision-making relating to group or regional IT security initiatives.

a) The information security program exists to protect Goodbaby's information and information systems

b) Information security's investment in processes, people and technologies will be proportionate with the value of the information and information systems at risk

c) Information security's approach to protecting information and information systems will comply with all necessary regional laws and regulations

d) Information security will address real and likely threats in a risk management driven approach

e) Information security services will benefit from service management principles

f) Information security will leverage internationally accepted cybersecurity standards and good practices

## 5. Information Security Approach

Although the specific IT security technologies, processes and procedures leveraged by Goodbaby International vary by subsidiary, the overarching IT security policies are uniform across the group and are summarized below.

### 5.1. Framework and Best Practice

Goodbaby International has adopted the Centre for Internet Security (CIS) Critical Security Controls in order to structure its approach to information security and adhere to international standards and best practice.

### 5.2. Acceptable Use Policy

An acceptable use policy will be maintained that describes how IT resources should be used by employees. All new employees are required to read and sign this policy as part of the onboarding process.

### 5.3. Access Control

#### 5.3.1. User Authentication

When connecting to the network, access requires a username and password. The strength of the password will be enforced and passwords will be updated on a regular basis.

#### 5.3.2. Remote Access

Access from remote locations (i.e. a location that is not a dedicated Goodbaby International office) requires use of a VPN solution, secured with multi-factor authentication (MFA), to access internal company systems.

#### 5.3.3. Business Critical Cloud Services

Access to business critical services hosted in the cloud, for example Office 365, will be secured with MFA when connecting from remote locations.

#### 5.3.4. Physical Access Controls

Data centres, server rooms and network cabinets will be locked at all times and access provided only to necessary IT engineers and support staff. Use of card- or dongle-controlled access into buildings is recommended.

### 5.4. Data Backup and Recovery

Daily backups of critical data, systems and servers will be conducted.

### 5.5. Security Awareness and Training

IT security policies will be shared with all employees. New employees will be briefed during the onboarding process and training sessions will be conducted via e-learning platforms or classroom-based training. These sessions will inform employees of their obligations towards the company with respect to information security, as well as train employees to identify social engineering (phishing) attacks.

### 5.6. Systems and Communication Protection

#### 5.6.1. Endpoint Protection

All endpoints (servers and workstations) will have, as a minimum, anti-virus and endpoint detection and response (EDR) software installed.

#### 5.6.2. Data Loss Prevention

Controls will be implemented to restrict: the use of cloud storage services to approved providers; the use of removeable media (e.g. USB) to authorised encrypted devices; the maximum email attachment size.

#### 5.6.3. Data Encryption

Controls will be implemented to ensure the encryption of corporate data at rest and in-transit in alignment with the Data Protection Policy.

### 5.7. Security Incident Management

Security incident response procedures will be maintained that define the response actions to be taken following different types of security incidents.

All employees must report any system vulnerabilities, incident or event pointing to a possible incident to the Service Desk as quickly as possible but no later than 24 hours of discovery.

## 6. Risk Management Plan

To protect the confidentiality, integrity, and availability (CIA) of Goodbaby's data in compliance with applicable regulations, Goodbaby IT has formal cybersecurity risk management processes based on ISO27005 and NIST 800-30. Goodbaby uses a formal Information Security Risk Management process that identifies risks and implements plans to address and manage them, which includes managing exceptions to the Information Security Policy and the risk acceptance process.

### 6.1. Identified IT Risks

The following risks have been identified as potential threats to Goodbaby International's IT infrastructure and systems.

- **Cybersecurity Incidents**: Ransomware, malware, or data breaches.
- **IT Hardware Failures**: Server, storage, or networking equipment failure.
- **Power Outages**: Loss of power impacting IT systems and data centers.
- **Natural Disasters**: Floods, fires, or earthquakes affecting data centers and critical IT infrastructure.
- **Human Error**: Accidental deletion or modification of critical data or misconfigurations.
- **Application Downtime**: Critical software failures due to bugs or misconfigurations.
- **Third-Party Failures**: Disruptions caused by service providers, including cloud, backup, and telecommunications services.

### 6.2. Preventative Actions

To minimize risks and prepare for disruptions, the following preventive measures are implemented:

- **Cybersecurity Measures**: Multi-factor authentication (MFA), encryption, and network security controls to reduce exposure to cyber threats.
- **Redundancy in Infrastructure**: Use of redundant servers, network links, and power supplies in key data centers.
- **Data Backup Strategies**: Follow the Data Backup and Recovery Policy regular backups of all critical data to offsite locations and cloud environments.
- **Routine Maintenance**: Regular maintenance and upgrades of hardware and software to prevent failures.
- **Service-Level Agreements (SLAs)**: SLAs with critical service providers to ensure minimal service disruption and prioritized response.

### 6.3. Contingency Plans for IT

In the event of a disruption, contingency plans will include:

- **Data Center Failover**: Activate secondary data centers with mirrored infrastructure for critical services.
- **Cloud-based Recovery**: Shift to cloud-based services for critical applications if on-premises systems fail.
- **Remote Access Enablement**: Ensure employees can access IT systems securely from remote locations if offices are affected.
- **Third-party Services**: Use third-party backup and disaster recovery providers to ensure continued access to IT resources.

## 7. Business Impact Analysis

### 7.1. Critical IT Services and Applications

The following IT systems and applications are identified as critical to business operations and must be prioritized for recovery:

- **Enterprise Resource Planning (ERP)**: Core business application for financials, procurement, and supply chain management.
- **Customer Relationship Management (CRM)**: Application used for managing customer interactions and sales processes.
- **Email and Collaboration Tools**: Microsoft Exchange, Office 365, and Microsoft Teams for business communication.

- **Web based Platforms**: Online platforms critical for customer interaction and sales.
- **Manufacturing Systems**: IT systems supporting production lines and inventory management.
- **Supply Chain Management Software**: Applications tracking the flow of goods and materials from suppliers to customers.

### 7.2. Impact of IT Disruption

The impact of IT disruptions will vary based on the type and duration of the outage:

- **Financial Losses**: Prolonged system downtime may lead to lost sales and missed opportunities.
- **Operational Disruption**: Inability to access critical systems could halt business processes such as manufacturing, customer service, and order fulfillment.
- **Reputational Damage**: Extended outages may affect customer confidence and brand image.
- **Regulatory and Compliance Issues**: IT disruptions could result in violations of data protection regulations (e.g., GDPR), leading to legal penalties.

### 7.3. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

Identify the RTO based on Service Level Agreement and RPO based on Backup and Recovery Policy.

## 8. Supporting Policies

Policies and standards are crucial to establishing, maintaining and monitoring proper information security practice. The Group Information Security Policy is underpinned by the following additional IT security policies:
*Acceptable Use Policy / Data Protection Standards Policy / Access Control Policy/ Asset Management Policy / Configuration Management Policy / Data Backup and Recovery Policy / Privileged Account Management Policy / Security Awareness and Training Policy / Security Incident Management Policy / Security Monitoring Policy / Systems and Communication Protection Policy / Vulnerability Management Policy*

## 9. Ownership and Approval

Under the direction of the Goodbaby International Board, the VP Group IT Systems & Services and the Director Group IT Security are responsible for ensuring compliance with this policy.