## Company Data Security Policy

### Overview & Objective:

Our company's data security policy details the rules and procedures for safeguarding our data and technology infrastructure.

As we increasingly depend on technology to gather, store, and handle information, we also become more exposed to serious security threats. Mistakes by individuals, cyberattacks, and system failures could result in significant financial losses and harm our company's reputation.

For this reason, we have instituted several security precautions. Additionally, we have provided guidelines that aim to minimize security risks. Both have been outlined in this policy.

### Coverage:

This policy is applicable to all employees, contractors, volunteers, and anyone with either long-term or short-term access to our systems and devices.

### Policy Components:

### Sensitive Information

Sensitive information is confidential and valuable. Some common examples include:

- Financial data not yet made public
- Customer/partner/vendor information
- Intellectual property, such as patents or new inventions
- Lists of customers (both current and potential)

All employees are required to safeguard this information. This policy provides instructions for employees to help prevent security breaches.

### Safeguard Personal and Company Devices

When employees use digital devices to access company emails or accounts, they potentially introduce security vulnerabilities to our data. We recommend that employees ensure the security of both personal and company-issued computers, tablets, and smartphones by following these steps:

- Secure all devices with strong passwords.
- Install and regularly update comprehensive antivirus software.
- Avoid leaving devices exposed or unattended.
- Keep browsers and systems updated monthly or as soon as updates are released.
- Access company accounts and systems only through secure and private networks.

### Protect Emails

Emails are common carriers of scams and harmful software (e.g., worms). To prevent virus infections or data theft, we advise employees to:

- Avoid opening attachments or clicking on links unless the content is clearly explained (e.g., “check out this amazing video”).
- Be cautious of clickbait headlines (e.g., prize offers or unsolicited advice).
- Verify the sender’s email and name to confirm authenticity.
- Look for signs of fraud or mistakes (e.g., grammar issues, unnecessary capital letters, or excessive exclamation points).

If employees are unsure about the safety of an email, they should consult our [IT Specialist].

**Manage Passwords Securely**

Password breaches pose significant threats to our infrastructure. Passwords must be both secure and kept confidential to avoid potential hacking. Employees should follow these guidelines:

- Choose passwords with at least eight characters, including uppercase and lowercase letters, numbers, and symbols. Avoid using easily guessed information (e.g., birthdays).
- Memorize passwords rather than writing them down. If writing is necessary, ensure the document (paper or digital) is kept confidential and destroyed after use.
- Only share credentials when absolutely necessary. If in-person exchange is not feasible, use the phone instead of email and ensure the person you're speaking to is recognized.
- Change passwords every two months.

Managing multiple passwords can be challenging. We will provide access to a password management tool that generates and securely stores passwords. Employees are required to set a secure password for this tool, following the same guidelines.

**Transfer Data Safely**

Transferring data carries inherent security risks. Employees must:

- Avoid transferring sensitive information (e.g., customer data, employee records) unless absolutely necessary. For large data transfers, employees should seek assistance from our [Security Specialists].
- Share confidential information only through the company network/system and avoid public Wi-Fi or personal connections.
- Confirm that the recipient of the data is authorized and follows proper security protocols.

**Report Scams, Privacy Breaches, and Hacking Attempts**

### Additional Measures

To further reduce the risk of security breaches, employees should:

- Turn off screens and lock devices when stepping away from their desks.
- Report stolen or damaged equipment to the [HR Department] immediately.
- Change all account passwords promptly if a device is stolen.
- Report any suspected threats or weaknesses in the company's security systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on company devices.
- Avoid visiting suspicious websites.

### Disciplinary Action

We expect employees to follow this policy diligently. Any breach of security protocols may result in disciplinary action:

- **First-time, unintentional, small-scale breaches**: A verbal warning may be issued, and the employee will undergo security training.
- **Intentional, repeated, or large-scale breaches** that cause significant financial or other damages will result in more severe disciplinary actions, up to and including termination.

Each incident will be assessed on a case-by-case basis.

### Take Security Seriously

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