**Company Cyber Security Policy**

**PURPOSE**

Our company's cyber security policy lays out our policies and procedures for safeguarding our data and technology infrastructure.

We grow increasingly vulnerable to major security breaches the more we rely on technology to collect, store, and manage information. Human errors, cyber assaults, and system failures could result in significant financial losses and harm our company's reputation.

As a result, we've put in place a number of security precautions. We've also put up some instructions that can be useful in reducing security threats. Both provisions are described in this policy.

**ELIGIBILITY**

All contractors, volunteers, and staff who have active or passive access to our data are subject to the Company Cyber Security Policy.

**POLICY COMPONENTS**

**Confidential Data**

Confidential information is both private and valuable. Here are a few examples:

- Unreleased financial data

- Information on customers, partners, and vendors

- Patents, formulas, and new technology are all examples of this.

- Customer databases (existing and prospective)

This data must be protected by all employees. We will give our staff guidance on how to avoid security breaches under this policy.

**Protect Company and Personal Devices**

Employees who access company emails or accounts using their own digital devices put our data at risk. We encourage our employees to keep their personal and company-issued computers, tablets, and phones safe. They'll be able to do this if they do the following:

- Make certain that all of your electronic devices are password-protected.

- Select and upgrade a comprehensive antivirus program.

- Make sure kids don't leave their devices alone or exposed.

- Install browser and system security updates on a monthly basis, or as soon as they become available.

- Only use secure and private networks to access company accounts and systems.

We also educate our staff to avoid using other people's devices to access internal systems and accounts, as well as lending their own devices to others.

When new employees acquire company-issued equipment, they will be given instructions on how to do the following:

- [Setup disk encryption]

- [Setup of a password management tool]

- [Antivirus/anti-malware software installation]

To protect their devices, users should follow the instructions and contact our [Security Specialists/ Network Engineers] if they have any questions.

**Keep your emails secure.**

Email is routinely used to send scams and dangerous viruses (e.g. worms). To avoid contracting a virus or having their personal information stolen, we advise our staff to:

- When the material is not well explained avoid opening attachments and clicking on links (e.g. "watch this movie, it's wonderful").

- Be wary of clickbait titles (e.g. offering prizes, advice.)

- Verify the email address and name of the person from whom they received a message.

- Keep an eye out for irregularities or freebies (For example, grammatical errors, capital characters, and an overabundance of exclamation marks.)

- If an employee has any doubts about the security of an email they received, they can contact our [IT Specialist.]

**Keep track of your passwords.**

Password breaches are serious because they put our entire infrastructure at risk. Passwords should not only be secure so that they cannot be readily hacked, but they should also be kept private. As a result, we encourage our employees to do the following:

- Choose passwords of at least eight characters (containing capital and lower-case letters, digits, and symbols) and avoid readily guessed information (e.g. birthdays.)

- Instead than writing down passwords, remember them. If employees must write their passwords on paper or in a digital format, they must keep the paper or digital document secure and destroy it once their work is completed.

- Only share credentials if it's really essential. Employees should use the phone instead of email when exchanging information in person isn't practicable, and only if they know the individual they're speaking with.

- Every two months, they should change their passwords.

It can be difficult to remember a big number of passwords. We'll pay for the services of a password manager that creates and stores passwords. Employees must use the above-mentioned guidelines to build a safe password for the tool itself.

**Secure data transfer**

Data transfer entails a security risk. Employees are required to:

- Only move sensitive data (for example, client information or staff records) to other devices or accounts if absolutely essential. When a large amount of data needs to be transferred, we ask staff to contact our [Security Specialists] for assistance.

- Share sensitive information via company network/system rather than public Wi-Fi or a private connection.

- Verify that the data recipients are appropriately authorized individuals or organizations with adequate security practices.

- Inform others of frauds, data breaches, and hacking efforts.

So that our [IT Specialists/ Network Engineers] can better defend our infrastructure, they need to be aware of frauds, breaches, and viruses. As a result, we encourage our staff to report any suspected assaults, suspicious emails, or phishing efforts to our specialists as soon as possible. Our [IT Specialists/ Network Engineers] must investigate immediately, repair the problem, and, if necessary, issue a companywide notice.

Our Security Specialists are in charge of training employees on how to recognize and avoid scam emails. Our staff are encouraged to contact them with any queries or concerns.

**Additional Measures**

We also tell our employees to do the following to limit the chances of a security breach:

- When they leave their desks, they should turn off their screens and lock their gadgets.

- Please notify [HR/ IT Department] as soon as possible if your equipment has been stolen or destroyed.

- When a device is stolen, change all account passwords at once.

- Report a looming threat or a potential security flaw in your company's systems.

- Avoid installing any questionable, unauthorized, or unlawful software on company computers.

- Accessing questionable websites should be avoided at all costs.

- Our staff must also follow our social media and internet usage policies.

Our [Network Administrators/Security Specialists] should:

- Firewalls, anti-malware software, and access authentication systems should all be installed.

- Arrange for all workers to receive security training.

- Inform your staff on a regular basis about new scam emails or viruses, as well as how to avoid them.

- Conduct a thorough investigation of security breaches.

- As other employees, you must adhere to the policies' terms.

To protect information, our organization will have all physical and digital barriers in place.

**Employees who work from home**

This policy's guidelines must also be followed by remote personnel. Because they will be accessing our company's accounts and systems from afar, they must adhere to all data encryption, protection standards, and settings, as well as ensuring the security of their private network.

We invite them to consult with our [Security Specialists/IT Administrators.]

**Disciplinary Procedures**

We expect all of our employees to adhere to this policy at all times, and those who violate it may face disciplinary action:

- In the event of a first-time, inadvertent, small-scale security breach, we may offer a verbal warning and security training to the employee.

- Intentional, frequent, or large-scale breaches (that result in significant financial or other harm): We will take more severe disciplinary action, including termination.

On a case-by-case basis, we will investigate each event.

Employees who are found to be disobeying our security guidelines will be subjected to progressive discipline, even if their actions have not resulted in a security breach.

**Take safety very seriously.**

Everyone should feel protected with their data, from our customers and partners to our employees and contractors. The only way to earn their trust is to protect our systems and information ahead of time. We can all help by being attentive and keeping cyber security at the forefront of our minds.