Policy Template : Cyber Security

a) PURPOSE

i) Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

ii) In today's world more and more of our business is conducted online, it is vast and growing. The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. A cyber-attack does not only directly threaten our company's confidential data, it may ruin the relationships with customers, and cause severe legal jeopardy to them and our company's reputation.

b) SCOPE

i) This policy applies to all our employees, contractors, volunteers remote or onsite, and anyone who has permanent or temporary access to our systems and hardware.

c) POLICY ELEMENTS

i) The company has outlined security measures that may help mitigate cyber security risks.

(a) Confidential Data

(i) Confidential data is information for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the company, partners, affiliates, and customers. Common examples are:

(ii) Unpublished financial information

(iii) Credit Card Numbers

(iv) Data of customers/partners/vendors

(v) Human resources records

(vi) Patents, formulas, or new technologies

(vii) Data security is the responsibility of all employees

.

(b) Protect personal and company devices

(i) Employees should only access company's emails and systems on company issued devices. Employees also should not use company's devices and equipment to access personal emails, or accounts.

(ii) This is vital as ignoring these protocols can introduce security risk to company and personal data. We advise our employees to keep both their personal and company-issued equipment and devices secure.

(c) Here is how:

(i) Use strong (numbers, letters, and symbols) passwords on all devices.
(ii) Avoid opening email attachments or clicking links.
(iii) Be suspicious of clickbait titles (e.g. offering prizes, advice.)
(iv) Choose and upgrade a complete antivirus software.
(v) Never leave devices exposed or unattended.
(vi) Do not give out personal information on the phone or through email or text.
(vii) Install security updates of browsers and systems monthly or as soon as updates are available.
(viii) Log into company accounts and systems through secure and private networks only.

(ix) When you use a shared computer or a business's Wi-Fi connection, you do not know how secure the network really is. Use your own device and secured network instead.

d) MANAGE PASSWORDS PROPERLY

i) Passwords are the first line of defense against numerous internet attacks of the company data infrastructure; hence password leaks are dangerous. Passwords should be SS, secure and secret. Here are some tips to make and keep them that way:

ii) Choose passwords with at least _____ characters (including capital and lower-case letters, numbers, and symbols). Make your password a nonsense phrase. Long passwords are good; long passwords that include random words and phrases are better.

iii) Remember passwords instead of writing them down. If employees need to store a list of their passwords or a password hint sheet on their computer in a document file, name the file something random

iv) Do not reuse passwords

v) Exchange credentials only when necessary. When exchanging them in-person is not possible, use the phone and only is the other person is recognized and verified.

vi) Change their passwords every thirty days.

e) TRANSFER DATA SECURELY

i) Transferring data introduces security risk. Employees must:

ii) Avoid transferring sensitive data, if information must be transferred it must first be encrypted by manager or IT specialist.

iii) confidential data must only be shared over the company network/ system and not over public Wi-Fi or private connection.

iv) Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.

v) Store data in a shared drive that only authorized persons can access.

vi) Report scams, privacy breaches and hacking attempts

vii) Employees must report seeming attacks, suspicious emails, or phishing attempts as soon as possible to our specialists. Our specialist must investigate promptly, resolve the issue, and send a companywide alert when necessary.

f) ADDITIONAL MEASURES

i) To mitigate the possibility of security breaches, here are some additional defenses:

(a) Lock screens and devices when leaving desks.
(b) Report stolen or damaged equipment as soon as possible to HR.
(c) Change all account passwords when a device is stolen or compromised.
(d) Report a perceived threat or possible security weakness in company systems.
(e) Do not download suspicious, unauthorized, or illegal software on company equipment.
(f) Avoid accessing suspicious websites.

(g) We also expect our employees to comply with our social media policy.
(h) Our Network Administrators should:
(i) Install company approved firewalls, anti-malware software and access authentication systems.
(j) Arrange for security training to all employees.
(k) Inform employees regularly about new scam emails or viruses and ways to combat them.
(l) Investigate security breaches thoroughly.
(m) Follow this policies provisions as other employees do.

g) REMOTE EMPLOYEES

i) Remote employees are also obligated to follow all aspects of this security policy as they also will be using company's systems, equipment, and confidential data.
ii) Remote employees can request that a Network Administrator test the security of their home network.

h) DISCIPLINARY ACTION

i) All employees will pass a security training, as so we expect all our employees to follow this policy. Should an employee disregard this policy and cause security breaches they will be subject to disciplinary action:

(a) First-time, unintentional security breach: We may issue a verbal warning and up to termination base on the severity of the breach.
(b) Intentional, repeated, or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to lawsuit or arrest.
We will examine each incident on a case-by-case basis.

i) TAKE DATA SECURITY SERIOUSLY

i) We are all responsible for the security of the data we use. Our customers, partners, employees, and contractors should know 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 with our cyber security.