Blueprint Education - Cyber Security policy November 2024

Cyber Security Policy

Policy Brief & Purpose

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks, and system malfunctions could cause great financial damage and may jeopardize our company's reputation. For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

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

Policy Elements

1. **Confidential Data**
   Confidential data is secret and valuable. Common examples are:
   - Unpublished financial information
   - Data of customers/partners/vendors
   - Patents, formulas, or new technologies
   - Customer lists (existing and prospective)
2. **Device Security**
   Employees must:
   - Keep all devices password protected.
   - Utilise an approved and updated antivirus software.
   - Ensure they do not leave their devices exposed or unattended.

- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

3. **Email Safety**
   To avoid virus infection or data theft, employees should:
   - Avoid opening attachments and clicking on links when the content is not adequately explained.
   - Be suspicious of clickbait titles.
   - Check email and names of people they received a message from to ensure they are legitimate.
   - Look for inconsistencies or give-aways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks).
4. **Password Management**
   Employees should:
   - Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols).
   - Remember passwords instead of writing them down.
   - Exchange credentials only when absolutely necessary.
   - Change their passwords every two months.
   - Where appropriate we will use multi-factor authentication
5. **Data Transfer**
   Employees must:
   - Avoid transferring sensitive data to other devices or accounts unless absolutely necessary.
   - Share confidential data over the company network/system and not over public Wi-Fi or private connection.
   - Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.

6. **Incident Reporting**
   Employees should report perceived attacks, suspicious emails, or phishing attempts as soon as possible to our IT lead. Our IT lead will investigate promptly, resolve the issue, and send a company-wide alert when necessary.
7. **Training & Awareness**
   Regular training sessions will be implemented to keep employees informed about the latest security threats and best practices.
8. **Disciplinary Actions**
   Employees who cause security breaches may face disciplinary action, including termination, depending on the severity of the breach.

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.