**Acceptable Use Policy**

**Overview:**

**\*company\***  intentions for publishing the Acceptable Use Policy is to ensure that all employees are able to work in secure, appropriate environments.

The following guidelines are what **company** requests employees practice in order to maintain a safe working environment for all. These guidelines cover security for the technologies employees are responsible, to better secure the company’s assets.

These requirements are expected to be complied with by everyone in the company regardless of the department with no exceptions. If policies are violated, employees will be subjected to consequences.

Personal Technology

At **\*company\*** every employee is given a personal device to conduct work on. In order to ensure the security of our company and employees, we require employees to follow the guidelines listed below.

1. All employees are asked to log out of devices when stepping away from their computer or workspace.
2. All company devices should have user and password login credentials implemented.
3. User login credentials should be implemented based on the password policy mentioned below.
4. Password Guidelines: Password is at least 8 characters long, contains letters (upper and lowercase), numbers, and special symbols.
5. Employees should never share their company devices with other employees or personals regardless of the occasion.
6. Devices assigned by the company should only be used to conduct work and nothing in relation to personal affairs.
7. Do not connect to public networks with the company device.
8. Illegal/ unlawful activity conducted on any device is not permitted.
9. All data created and accessed using a company device is under company ownership.

User Accounts

Every employee in our company is assigned unique login credentials. In order to maintain a secure system, employees follow the following procedures listed below.

1. Never leave credentials unattended whether it be written down on paper or saving it in a place where others can gain access to it.
2. Never share credentials with other employees. Under no circumstance should credentials be shared for any type of work.
3. Change account login information at least once every 3 months. When creating a new password, make sure to follow password policy guidelines.
   1. Password Guidelines: Password is at least 8 characters long, letters (upper and lowercase), numbers, and symbols used.

Internet Use

All employees are given access to our networks along with a personal company email. We ask that all employees abide by the procedures requested below.

1. Do not share email credentials with anyone regardless of the person.
   1. In the event login credentials need to be shared for work related purposes, one time passcodes must be used and communicated either through phone or a platform where the passcode is deleted immediately after.
2. Never leave email credentials unattended.
3. Never access your company email from a public device.
4. Log out of your email account after each use.
5. Enable Two-Factor Authentication for account login.
6. Set up security questions and avoid using answers that may be predicted by others.
7. Change account login information at least once every 3 months. When creating a new password, make sure to follow password policy guidelines.
   1. Password Guidelines: Password is at least 8 characters long, containing letters (upper and lowercase), numbers, and special symbols.
8. Never leak company data through any form of media.
9. Any activity unrelated to work is not permitted.
10. Unlawful activity conducted through the company network or email is not permitted.
11. All activity conducted under the company’s network is under company supervision.

Should you have any questions or concerns regarding the statements of this policy, please contact your supervisor for additional details.