Kevin's CyberSecurity Team

Use of Technology Security Policy

October 2019

Mission:

Our mission is to protect and secure your assets from harmful cyber-attacks all around the world! Below are guidelines in order to prevent such an attack on your network and confidential system.

RULES:

Rule 1:
Keep your personal and company device with you at all times.

Rule 2:
Create a very complex password for your company email.

- Must be 8-12 characters long.
- Must contain at least special character (@#$)
- Must contain two uppercase letters.

Rule 3: Do not share your information with anyone!

- Do not share any passwords or information to anyone outside the company!

Rule 4:
Always log out and lock your device once you are done using it.

- Do not leave your device unlocked even for a brief minute.

Rule 5:
Do not download any unauthorized application(s) without the consent of a supervisor.

- Do not download any personal items on your company issued device.

Rule 6:
Please update your passwords every 30 days.

- Do not use any password close to the previous one. Must be totally different.

Rule 7:
Report to a supervisor or authorized personnel if someone has hacked or accessed your device and information immediately.

- Not doing so can result in termination.

Rule 8:
Report any software breaches to supervisor to authorized personnel immediately.

- Examples include virus or hackings of network.

Rule 9:
Do not access unsecured websites.

- Websites with “http” are not secured.

Rule 10:
Do not share any hardware material such as harddrive or USB flash drive with any unauthorized personnel.