Password Security

* Passwords must be at least 8 characters and include UPPERCASE letters, lowercase letters, numbers and symbols.
* Individuals should not share account or system passwords or login credentials.
* If an individual cannot access their system due to a password issue, contact the IT department to have it reset.

Email Security

* Individuals are not allowed to send personal emails or respond to non-authorized email accounts on company systems. No email that is not approved should contain confidential or sensitive company information.
* Abstain from opening attachments or clicking any links in the situations when its content is not well explained
* Make sure to always check email addresses and names of senders.
* Search for inconsistencies
* Be careful with clickbait titles (for example offering prizes, advice, etc.)

Information Security

* Individuals are not authorized to log onto company sites, servers or accounts unless from a secured and authorized system. Logging in from personal systems or devices is not recommended for security reasons.
* Individuals should not discuss confidential company information:
  + Outside of the work space
  + With individuals who do not have clearance to be privy to said information
  + In open spaces that can be easily overheard
  + Without first ensuring they are not otherwise being monitored in some way.

Technology Management

* All systems must be properly secured. Do not leave systems unlocked and unattended.
* If you turn away from your system, lock the screen.
* Please ensure all latest software updates are installed and that all requisite antivirus and anti-malware software is up to date.
* Any company device should only be logged onto through a safe and authorized network.

Social Media Policies

Individuals are not allowed to post sensitive information or information related to the company unless it is specific company events, promotions or company related public announcements.

Incident Management

Keep Policies up to date

All individuals are required to complete a mandatory cyber security refresher course every six months to be kept up to date on latest policies and changes as well as potential attacks and threats.