Acceptable Use

1. **General Use and Ownership:** Everyone should be aware that the information they create or store on company assets remains the sole property of [Company Name]. Because of the need to protect [Company Name]'s company assets, management cannot guarantee the confidentiality of personal information stored on any company assets. Employees, contractors, and / or third-parties are required to exercise good judgment regarding their reasonable, but limited, personal use of company assets.

   All employees, contractors and/or third parties are required to comply with the following statements:

   a. Secure your equipment: lock it up when not in use, put it in your trunk, don't leave it unattended.
   b. If your laptop is missing, contact security@[Company Name].com within two hours and file a police report within 24 hours.
   c. Don't turn off or alter security applications or settings on your equipment (e.g. HD Encryption, Antivirus or [Company Name]). Any exclusion needs to have a documented and approved Jira HelpDesk ticket.
   d. All endpoints must have a supported OS installed and patched. This includes the latest version of Mac/Windows/Linux OS.
   e. Don't change the computer name assigned to the [Company Name] issued device.
   f. Don't store Confidential or Restricted (See Data Classification table below) information on removable media, unless approved by Security or IT. Request approval by emailing help@[Company Name].com.
   g. If you are having problems with an application or want to know if you can install something, contact help@[Company Name].com.
   h. Don't probe, scan, or disrupt our networking technology stack. No denial of service attacks, no unauthorized wireless access points, you get the idea.
   i. Lock your computer screen when you are away from it.
   j. If equipped, enable location services for your devices.
   k. Don't let somebody else use your account credentials or badge/access card to access physical and/or digital workspace.
      i. If you're escorting visitors, be sure to scan your badge for each visitor.
   l. Don't create user accounts on your device for non [Company Name] persons.
   m. Don't reuse your passwords and do not use [Company Name] passwords for non [Company Name] sites (e.g. personal sites, social media sites, etc.).
   n. We get it, you have a lot of passwords. Using a password manager is a good security practice.
      i. Corporate passwords can be stored only in these password managers:
         1. Example Solution

2. Example Solution

o. Do not store corporate passwords in your personal password manager.
p. Don't leave sensitive information lying around on your desk, at printers, or on whiteboards.
q. If you leave [Company Name], all assigned equipment must be returned. All [Company Name] data must be left on the system and remains property of [Company Name].
r. Applications or plug-ins downloaded from the internet pose a risk to our environment. If you have a business need for an application or plugin, please use legitimate, known app stores (i.e. Apple App Store, Google Play App Store, Amazon App Store, Microsoft Store). (Use this section as applicable)
    i. If you have a business need to download an app from any other app store, please obtain pre-approval from the security team at security@[Company Name].com.
s. Users are responsible to review the features and functionality of an application and are not allowed to download applications that will collect Confidential or Restricted data. In addition, users are responsible to keep applications current by always applying the latest updates.
t. Users are responsible to ensure all downloaded applications are configured securely to protect the device and the data.
u. Do not allow others to enter into secured areas without scanning their access badge (no tailgating). If escorting a visitor through badged areas, scan your badge for both yourself and once for each of your visitors.
v. While on the [Company Name] network, do not connect any [Company Name]-issued device to a non-[Company Name] machine via VPN, SSH, or other remote access techniques to access a personal network. If you have a business need to access your personal network while at work, contact security@[Company Name].com for approval.

2. **Proprietary Information:** [Company Name]'s non-Public information and intellectual property (including trade secrets) are extremely valuable to [Company Name]. Treat them accordingly and do not jeopardize them through your business or personal use of company assets or other communications, including e-mail, instant messaging, text messaging, internet access, social media and phone conversations. All employees, contractors and/or third parties are required to comply with the following statements:
    a. All [Company Name] information should be classified according to the Data Classification and should be handled appropriately according to classification.
    b. Use software in accordance with license restrictions. Do not install pirated versions of any applications. e.g. Adobe CS; if you need a tool contact IT via help@[Company Name].com.
    c. All asset purchases to be used for [Company Name] purposes must be formally approved in advance. This includes but is not limited to: laptops or other

computing devices, software or subscriptions, domain names, certificates, and marketing or other identity-related materials.

d. Exporting software with encryption technology is subject to many laws, so consult Legal if you find yourself potentially exporting the [Company Name] product.
e. You are not allowed to attack or exploit any of our systems unless it is authorized in writing by the CISO. Contact security@[Company Name].com if you have questions or concerns about security vulnerabilities.
f. Don't share customer or employee lists without prior authorization.
g. Don't share source code or any other intellectual property without prior authorization.
h. Personal files may be sent electronically but files must either be unencrypted, or the Security team must be given the ability to decrypt the files to review the contents for proprietary information, if necessary.
i. The Security team reserves the right to review the contents of notes, physical or electronic, upon termination of employment.

3. **Appropriate Use of Email / Electronic Messaging:** Users should be aware that the information they create or store within company email or other electronic messaging may be monitored and reviewed.

   All employees and contractors are required to comply with the following statements:

   a. Don't spam anyone.
   b. Don't harass anyone.
   c. Don't use your [Company Name] email address outside of [Company Name] unless it is part of your job to do so.
   d. Never use your [Company Name] email in combination with your [Company Name] password to log into external, non-[Company Name] supported applications (e.g. LinkedIn, Facebook, Twitter).
   e. Extreme caution is to be used when opening e-mail attachments or clicking on links received from unknown senders, which may contain malware or be used to steal credentials and other information. Send suspicious emails to Security@[Company Name].com.

4. **Appropriate Use of Non-[Company Name] Assets (Bring Your Own Device):** Users should be aware that company resources and networks should be accessed via company owned devices.
   a. All employees and contractors are required to comply with the following statements:
   b. Your non-[Company Name] issued device can only be connected to the Guest wireless network. That means, don't plug it into the Ethernet jack in the wall either.

c. You are not allowed to VPN to our network from your non-[Company Name] device.
d. Employees and contractors may connect non-[Company Name] mobile devices to [Company Name] supported apps (e.g. Email, Calendar, Contacts).
e. Do not save or store company attachments locally on your non-[Company Name] device.
f. Non-[Company Name] assets that contain company information may be forensically analyzed and wiped.