## USB Removeable Media Checklist

#### Follow these guidelines for using and managing removable media and devices at work

**When to Use:**

* **Do NOT use USBs without prior permission** for work or at work
* **Avoid using removable media** whenever possible  
  + If you are using USBs currently in your role, work with the right people to securely transfer   
    any sensitive data to a secure drive and promptly delete the data from the device after finishing.
* **Never connect unknown media devices you’ve found** to a computer. Give any unknown storage   
  device to security or IT personnel.

**How to Protect:**

* **Disable Auto-run and Autoplay features** for all removable media or devices. These features automatically run when plugged into a USB port or drive.
* **Ensure anti-virus solution(s) are installed** on your computer to actively scan for malware when   
  any type of removable media or device is connected.
* **Ensure that all removable media and devices are encrypted.** This will render any data useless   
  to unauthorized users should the device be lost or stolen.
* **Always apply new passwords before and after any trip** where company data is being utilized   
  on removable media or device. Never disclose the passwords used with removable media or devices   
  to anyone.
* **Keep personal and business data separate.** Do not store work data on any personal device   
  and vice versa