**Bring Your Own Device Procedure**

The **[organization]** grants its employees use of personally purchased smartphones and tables at work for their convenience leveraging the Bring Your Own Device procedure. **[The organization]** reserves the right to revoke this privilege if users do not abide by the information outlined below.

# PurposeThe purpose of this procedure is to protect the security and integrity of [the organization’s] data and technology infrastructure.

# Scope

# All staff, employees and entities working on behalf of [the organization] operating their personally owned wireless devices on the [organization’s] wireless network are subject to this procedure.

# Procedure

Personally owned devices are permitted to access any **[organization]** network resource available on the public Internet. It is the employees’ responsibility to maintain their own device(s) and to ensure that proper malware/anti-virus software is operational. **[Organization]** does not manage applications and content on personally owned devices and the employee is personally liable for all costs associated with his or her device.

* A GUEST wireless network is available for personally owned devices. The GUEST network provides public internet access only. This does not provide access to the internal [organization] network.
* **[The organization]** prohibits the use of personally owned computers, tablets, smartphones and all other WiFi enabled devices on its SECURE network.
* Other devices connecting to the GUEST Network are not necessarily **[organization]** property and may not have sufficient, appropriate or up-to-date anti-virus software installed and running. Connecting to the GUEST Network may expose a device to an infected device. The user assumes all risk when using the GUEST Network. **[Organization]** assumes no liability for damage or loss of data incurred while using the GUEST Network.

# Enforcement

This procedure is for your protection. Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

* **[Organization]** reserves the right to disconnect devices or disable services without notification.
* **[Organization]** employees and visitors are expected to use personal devices in an ethical manner at all times and to adhere to **[organization]** Administrative Regulation 3600.
* **[Organization]** devices may be remotely wiped if:
	+ The device is lost
	+ The employee terminates his or her employment
	+ IT detects a data or procedure breach
	+ Other security risks are identified
* It is an employee’s responsibility to take additional precautions such as backing up email, contacts and other important information in the event that IT must remotely wipe the device.

# Exceptions

Limited exceptions to the procedure must be approved **[organization.]**

**[Organization]** employees must agree to the terms and conditions set forth in this procedure in order to be able to connect their devices to the company network.

1. **Definitions**
* Not applicable at this time