1.0 Purpose
This policy provides for more secure Bluetooth Device operations. It protects the company from loss of Personally Identifiable Information (PII) and proprietary company data.

2.0 Scope
This policy covers all <Company Name> Bluetooth Devices.

3.0 Policy

3. 1Version level
No Bluetooth Device shall be deployed on <Company Name> equipment that does not meet Bluetooth v2.1 specifications without written authorization from the InfoSec Manager. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

3.2 Pins and Pairing
When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area. If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, **you must refuse the pairing request and** report it to InfoSec, through your Help Desk, immediately. Unless your Bluetooth device itself has malfunctioned and lost its pin, this is a sign of a hack attempt.

3.3 Device Security Settings
All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
If your device allows the usage of long PIN's, you must use either a 13 alphabetic PIN or a 19 digit PIN (or longer).
Switch the Bluetooth device to use the hidden mode, and activate Bluetooth only when it is needed.
Update the device's firmware when a new version is available.
3.4 Security Audits
InfoSec shall perform audits to ensure compliancy with this policy. In the process of performing such audits, InfoSec shall not eavesdrop on any phone conversation.

3.5 Unauthorized Use
The following is a list of unauthorized uses of <Company Name>-owned Bluetooth devices:

- Eavesdropping, device ID spoofing, DoS attacks, or any for of attacking other Bluetooth enabled devices.
- Using <Company Name>-owned Bluetooth equipment on non-<Company Name>-owned Bluetooth enabled devices.
- Unauthorized modification of Bluetooth devices for any purpose.

3.6 User Responsibilities

- It is the Bluetooth user's responsibility to comply with this policy.
- Bluetooth users must only access <Company Name> information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to InfoSec.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**

6.0 Revision History

Version	Author	Update Comments