

**MICHIGAN STATE UNIVERSITY
HEALTHTEAM
POLICIES/PROCEDURES**

SUBJECT: Wireless Device Security	NO. IS -6
SCOPE: MSU HealthTeam Faculty, Staff and Contract Supported Users	PAGE: 1 of 1
AUTHOR:	
Final Approval: Practice Executive Committee	
EFFECTIVE DATE: 1/15/2005	REVIEW DATE: 1/2006, 1/2007, 1/2008

POLICY STATEMENT

Wireless implementations must maintain point to point encryption and employ strong user authentication and authorization that checks against user name and password.

All Wireless Devices are recommended to use some form of VPN software when connecting to PHI systems.

PROCEDURE

**Department
Head/Supervisor**

1. Any device that is purchased/utilized by the department that has the ability to communicate 'wirelessly' will be configured correctly prior to accessing the HealthTeam network.
 - a. Ensure that the Information Services department has the opportunity to review the configuration of the wireless device prior to authorizing its use by the department staff.
 - b. If there is doubt regarding whether the device is properly configured, ensure the device is powered off until such time as it's proper configuration can be confirmed.
 - c. Under no circumstances should a device be utilized (even for short periods of time) if it is not approved by the IS staff.
2. Coordinate the purchase of wireless devices through the IS staff to ensure it meets the current standards.

**Information Services
Staff**

3. Upon request of a department, verify their wireless devices have the Virtual Private Network software installed and properly configured.
 - a. Randomly perform checks to verify all wireless users have been authenticated to the HealthTeam network.
 - b. Report any violations to the appropriate IS Manager.
 - c. Use any means available to shut-down or disable any unauthorized access to the Wireless network and identify the source of the access.