Stony Brook University
Computer Science

Wireless Communication Policy

CS Department Wireless Communication Policy

1.0 Purpose
This policy prohibits access to SUNY Stony Brook CS department networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by DOL are approved for connectivity to SUNY Stony Brook CS department's production networks.

2.0 Scope
This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of SUNY Stony Brook CS department's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to SUNY Stony Brook CS department′s production networks and labs outside the DMZ do not fall under this policy.

3.0 Policy
To comply with this policy, wireless implementations must: Maintain point to point hardware encryption of at least 56 bits. Maintain a hardware address that can be registered and tracked, i.e., a MAC address. Support strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

4.0 Enforcement
Any user found to have violated this policy may be subject to disciplinary action.

5.0 Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History