a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #15
Wireless Networks

Introduction

1. UBC has a large and complex wireless network that plays an integral role in the operations of the University. Consequently, intruders and hackers may consider the wireless network an attractive target to breach the security of UBC Electronic Information and Systems.
2. This standard defines requirements to ensure that wireless devices, such as Wireless Access Points (WAPs), which allow wireless devices to connect to a wired network, are deployed in a secure, controlled and centrally managed way to reduce the likelihood of a security breach. Unless otherwise indicated, the UBC IT Infrastructure Team (the "Infrastructure Team") is responsible for ensuring compliance with this standard.
3. In addition to this standard, UBC IT wireless networks provisioned by UBC IT are governed by Policy 130, Management of the Wireless Network. In particular, all new WAPs must be authorized under the terms of that policy.
4. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Physical Protection

5. WAP hardware must be protected to ensure physical security mechanisms (e.g. locked cabinet, high ceiling mount, etc.) are in place to prevent theft, alteration, or misuse.

Secure Configuration

6. All WAPs should be secured using Wi-Fi Protected Access (WPA2) with a minimum of AES 128-bit encryption.
7. Wired Equivalent Privacy (WEP) is prohibited for wireless network security, as it is insecure.
8. It is recommended that Users connecting to WAPs, providing access to the UBC LAN, be configured to use the "autoconnect" ubcsecure automated client configuration tool. This will help prevent connecting to rogue WAPs, which have been setup with the same name (spoofing) to steal credentials.
9. Console access must be password protected in compliance with the Password and Passphrase Protection standard.
10. WAP and wireless controller management must be handled as follows:
    a. utilize secure protocols such as HTTPS, SSH, and CAPWAP;
    b. management must only be over the LAN interface;
    c. if SNMP is used in the management environment, all default SNMP community strings must be changed, otherwise it must be disabled;
    d. vendor defaults such as encryption keys, and administrative passwords must be changed.
11. The use of Telnet or other insecure protocols is prohibited.

Security Updates

12. The operating system or software code on WAP and wireless controllers should be patched and kept current to ensure proper protection from the latest security vulnerabilities.

Additional Wireless Requirements for Payment Card Industry (PCI) Information

13. Users responsible for Merchant Systems must:
    a. ensure that a perimeter firewall is in place between any wireless network and Merchant Systems processing Payment Card Industry (PCI) Information. These firewalls must be configured to deny or control any traffic from the wireless environment to Merchant Systems;

b. test for the presence of unauthorized WAPs on a quarterly basis. Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control NAC), or wireless IDS/IPS; and
c. Report any unauthorized WAPs as a security incident, in compliance with the Reporting Information Security Incidents standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Policy 130, Management of the Wireless Network

Password and Passphrase Protection standard

Reporting Information Security Incidents standard