PHAMBILI

WIRELESS NETWORK SECURITY POLICY

Contents

Overview

The major problem with wireless networks, and the main reason for this policy, is related to their open nature. People often don't realize, for example, how far their wireless network extends beyond the confines of their building; the propagation characteristics of radio waves mean there is limited control over where the signal associated with a wireless network is accessible from. This leads to a situation where, unlike wired networks, a hacker or malicious user can manipulate or eavesdrop on the network from uncontrolled locations, possibly beyond the geographic boundaries of the Municipality, which were not intended to be served when the network was implemented.

Wireless networks can also create "backdoors" to wired networks. Sundays River Valley Municipality, like many organizations, takes extensive measures to protect the integrity of its wired network and the data it contains. This includes the use of various levels of firewalls and access controls, virtual private networks, and other security-enhancing technologies. A single unauthorized or badly configured wireless access point connected to the Municipality's wired network has the potential to create a "backdoor" to the wired network, circumventing network security and thereby allowing a hacker to effortlessly bypass the restrictions that would normally be in place to limit the damage they can do.

Legislative References

- ISO 17799
- Information Security Forum (Code of good practice for Information Security)
- Minimum Information Security Standards
- International Standard for Risk Assessment
- COBIT Audit Framework
- The constitution of the republic of South Africa, 1996;
- The local Government: Municipal Systems Act, 2000(Act32 of 2000);
- The local Government: Municipal Finance Management Ac, 2003(Act 56 of 2003);
- State Information Technology Act, 1998 (Act 88 of 1998);
- Electronic and Communications Act, 2002 (Act 68 of 2002);
- Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000)
- Protection of Personal Information Act

Scope of the policy

This policy applies to all "wireless capable" devices owned by the Municipality, attached to any part of the Municipality's network, or operated on any part of the Municipality's campus. It should be interpreted such that it has the widest application. In particular, references to the Information Technology Division should, where appropriate, be taken to include departmental or other system managers responsible for the provision of a computing or communication service.

A wireless capable device is one that can make use of radio frequency transmissions to connect to a local area Internet Protocol network. This network may or may not be connected to Sundays River Valley Municipality' wired network infrastructure. It includes, but is not limited to, devices conforming to IEEE the 802.11 (WLAN) and 802.15 (Bluetooth) series of specifications.

The use of commercially available wireless services operating in a licensed frequency band to connect to a value added network services provider (such as the use of VSAT or GPRS through a cellular telephone), provided they operate in isolation from Sundays River Valley Municipality' local area network, are specifically excluded from this definition and by implication from this policy. In these cases, other provisions in the acceptable use policy may still apply.

In cases where this policy makes specific reference to features provided by the 802.11 specification, it is assumed that devices making use of other technologies will use the equivalent features in their technology. In the event of uncertainty about a particular technology (for example where no comparable features exist) queries regarding the interpretation of this policy with respect to other wireless technologies should be addressed to the Information Technology Division.

General provisions

All wireless capable devices must be approved by ICASA or its nominee for use in South Africa. This includes obtaining an appropriate radio frequency license or specific exemption from licensing (such as type approval). Devices should only be operated within the bounds of their licensing or type approval.

All wireless capable devices connected to or making use of Sundays River Valley Municipality' network infrastructure should be registered with the Information Technology Division. Such registrations should indicate whether the device is a wireless access point, bridge or client.

All wireless clients connecting to the Municipality's network should associate with an access point and all access points should operate in 802.11 "infrastructure" mode. No 802.11 "ad-hoc" or informal networks are to be connected to the Municipality's network.

Service Set IDs (SSIDs) and network names, whether broadcast in beacon frames or not, must be approved by the Information Technology division prior to being used on Sundays River Valley Municipality' campus. Once registered as per paragraph 3.2, SSIDs may not be altered without the approval of the Information Technology Division.

Channel/frequency allocation on wireless access points and devices should be done so as to minimize interference with other wireless services on campus. In general, devices with the ability to automatically select the best channel should be configured to use this feature. However, it may be necessary to consult with the Information Technology Division to determine what channels are available in a particular area.

Wireless devices should be configured to make use of the minimum possible radio transmission power in order to achieve their objective and coverage area.

All wireless access points used on campus should conform to a set of minimum specifications as published from time to time by the Information Technology Division. These specifications are intended to maintain the security and interoperability of wireless devices on campus.

No access to the Municipality's financial, human resources, Employee records or other sensitive data will be made available via wireless access. This includes, where applicable, departmental records.

Any exceptions to the general provisions set out above must be approved by the Director of Information Technology.

Register Access Points

1. All wireless Access Points connected to the network must be registered and approved by SRVM.
2. All approved Access Points are subject to periodic penetration tests and audits.

Approved Technology

All wireless LAN hardware implementations shall utilize Wi-Fi certified devices that are configured to use the latest security features available.

Physical Location

1. Security mechanisms should be put in place to prevent the theft, alteration, or misuse of
2. All devices shall be locked and secured in an appropriate manner.

Configuration

1. The default SSID and administrative username / password shall be changed on all Access Points. Device management shall utilize secure protocols such as HTTPS and SSH. If SNMP is used in the management environment, change all default SNMP community strings, otherwise disable it.
2. Access Points should be placed strategically and configured so that the SSID broadcast range does not exceed the physical perimeter of the building. If configurable, adjust the SSID beacon transmission rate to the highest value. Console access shall be password protected.

Authentication and Transmission

- All wireless access points that connect clients to the internal network (LAN) shall require users to provide unique authentication over secure channels and all data transmitted shall be encrypted with an approved encryption technology.

Internet-only Deployments

Access Points deployed to provide Internet-only service shall be separated from the internal network by denying all internal services. Access Point / Base Station management shall be limited to internal or console users and not available to wireless clients.

Peer-to-peer and personal area networks

Temporary peer-to-peer, personal area or "ad-hoc" networks may be created provided:

1. They do not interfere with other wireless services provided by the Municipality;
2. They do not connect to the Municipality's network in any way;
3. They are for personal use.
4. Provided that the SSID contains the user's Sundays River Valley Municipality username in an easily distinguishable way, no specific approval is required for such networks.

Since "ad-hoc" networks provide little in the way of access controls, anyone creating such a network should be aware that they may be exposing the entire contents of their computer to anyone within range of their network. As such, users should take appropriate precautions to ensure that no sensitive or confidential information (such as exam papers or financial records) is made available in this way.

Temporary hot spots

It is sometimes necessary to set up additional wireless access points for testing purposes or to handle unusual demands (for example during conferences). In these instances, it is permissible to create temporary wireless "hot spots" provided that, in addition to the general requirements set out above, they meet the following criteria:

1. The temporary hot spot, as well as any access points or other wireless infrastructure used in its creation, may not operate for a period in excess of two weeks. It is intended that this provision is used for short term, once off installations rather than for ongoing, ad-hoc type arrangements.
2. No wireless infrastructure may be permanently affixed.
3. All access points and wireless clients making use of the hot spot shall make use of some form of standards-based encryption. At a minimum, this means that the use of Wired Equivalent Privacy (WEP) should be an enforced, mandatory requirement for clients connecting to an access point.
4. The SSID advertised by the hot spot must be unique and differ from any SSID in use for permanent installations.

5. Users of any network subnet temporarily hosting a wireless hot spot should be made aware of the privacy implications of hosting such a hot spot on their subnet. This could be done, for example, by sending e-mail to an appropriate distribution list.

Permanent installations

The wireless network will be logically segregated from the wired network and subject to specific access controls. For this reason, it is necessary to consult with the Information Technology Division prior to installing access points in order to ensure that the supporting network infrastructure is capable of such segregation. Users planning wireless installations should be aware that not all parts of the Municipality's network are capable of such segregation.

In order to ensure that wireless access points are correctly configured and able to inter-operate with the Municipality's network, all access points should be installed and maintained by, or in consultation with, the Information Technology Division.

1. All permanent wireless installations shall be configured in accordance with a set of guidelines and best practices published from time to time by the Information Technology Division. These guidelines will cover topics such as network naming, IP address allocation, encryption and authentication.
2. All wireless clients must make use of appropriate, up-to-date anti-virus software. In addition, the use of personal firewall software on wireless clients is highly recommended.
3. Users should be aware of the privacy concerns relating to wireless networks and should take extra care to ensure that sensitive information is not transmitted over the wireless network.

Other considerations

Recognizing that, in general, wireless networks provide significantly less bandwidth than their wired counterparts and that this bandwidth is shared amongst all users of a particular wireless access point, users should ensure that they are considerate in their use of the wireless network. This means, for example, that using the wireless network to stream high quality full motion video or for any other high-bandwidth application could be seen as a contravention of the acceptable use policy.

Audience and Applicability

The wireless network security policy is applicable to everyone in the Municipality who has access to the ICT services and network infrastructure of the Municipality.

Responsibilities of the Municipal Manager

The Municipal Manager at the advice of the Senior Systems Administrator can make a determination on the following:

1. Review of the wireless network security policy,

2. Change the wireless network security policy if it is not compliant with information security legislation,
3. Propose amendments and and/or deletions on the guidelines,

Responsibilities of the IT Manager

1. The Senior Systems Administrator is responsible for the assessing and evaluating of the risk on the accessing of the abuse or miss-use of affected computer systems.
2. Appropriate rights or revocation thereof of those rights to the Municipal employees violating the wireless network security policy,
3. Ensure that the wireless network security policy is effective and user friendly.

Escalation Procedure

1. The system maintenance employee shall escalate any deviations or violation of the wireless network security policy to the Systems Administrator.

2. The Systems Administrator after evaluating the merits of the violation and the extent of the violation shall report the violation or breach to the IT Manager.

3. The Senior Systems Administrator shall immediately issue a directive to the Systems Administrator to suspend the Use of certain devices to institute a formal and proper investigation.

4. On the outcome of the investigation, the Senior Systems Administrator shall inform the Municipal Manager of such for a ruling or further investigation upon which a decision shall be taken on the necessary course of action.

5. The Senior Systems Administrator may allow deviation only on the basis of an operation that requires such an intervention.

6. The Municipal Manager may approve or decline such request for a deviation.

Policy Compliance

Compliance Measurement

The IT Section team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exceptions to this Policy must be approved in writing by the Municipal Manager.

Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. IT Section reserves the right to restrict any device or connection that does not comply with this policy.

Reporting & Disclosure Requirements

The Senior Systems Administrator shall report from time to time the management, administration and operationalization of the policy implementation to the Municipal Council.

Policy Reviewal

This Policy will be reviewed annually.

APPROVED BY COUNCIL ON 08 JULY 2022

.... 08 JULY 2022

S H RUNE
MAYOR