# Metro Wireless NETWORK SECURITY POLICY v1.33

## 1 Introduction

1.1 This document defines the Network Security Policy for Metro Wireless International Inc. (referred to hereafter as the MWI). The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support and are Customers of the network.

1.2 This document:

a. Sets out MWI's policy for the protection of the confidentiality, integrity and availability of the network;
b. Establishes the security responsibilities for network security;
c. Provides reference to documentation relevant to this policy.

1.3 The network is a collection of communication equipment such as routers, radios, switches, etc. which has been connected by cables or wireless devices. The network is created to share Internet bandwidth, private networking services, voice services and other customer services.

## 2 Purpose/Scope of this Policy

2.1 The purpose of this policy is to ensure the security of MWI's network. To do this MWI will:

a. Ensure Availability
Ensure that the network is available for Customers;
b. Preserve Integrity
Protect the network from unauthorised or accidental modification.
c. Preserve Confidentiality
Protect assets against unauthorised disclosure.

2.2 The purpose of this policy is also to ensure the proper use of MWI's network and make Customers aware of what MWI deems as acceptable and unacceptable use of its network.

2.3 Willful or negligent disregard of this policy may be investigated and dealt with under MWI Disciplinary Procedure.

2.4 This policy applies to all networks managed by MWI used for:

- Internal office users and staff of MWI.
- MWI's networks across all geographical locations.
- MWI's network as it pertains to type 2 access over another provider network.
- All other applicable networks accessed by MWI staff or representatives.

## 3 The Policy

3.1 The Network Security Policy for MWI is described below:

MWI information network will be available when needed and can be accessed only by legitimate customers or employees. The network must also be able to withstand or recover from threats to its availability, integrity, and confidentiality. To satisfy this, MWI will undertake the following:

a. Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
b. Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
c. Implement the Network Security Policy in a consistent, timely and cost-effective manner.
d. Where relevant, MWI will comply with:

FOIA - (Freedom of Information Act)
EIR -(Environmental Information Regulations)
NIST - (National Institute of Standards and Technology)
CIS - Controls (Center for Internet Security Controls)
ISO - (International Organization for Standardization)
HIPAA - (Health Insurance Portability and Accountability Act) / HITECH Omnibus Rule
PCI-DSS - (The Payment Card Industry Data Security Standard)
GDPR - (General Data Protection Regulation)
CCPA - (California Consumer Privacy Act)
AICPA - (American Institute of Certified Public Accountants)
SOX - (Sarbanes-Oxley Act)
COBIT - (Control Objectives for Information and Related Technologies)
GLBA (Gramm-Leach-Bliley Act)
FISMA - (Federal Information Security Modernization Act of 2014)
FedRAMP - (The Federal Risk and Authorization Management Program)
FERPA - (The Family Educational Rights and Privacy Act of 1974)
ITAR - (International Traffic in Arms Regulations)
COPPA - (Children's Online Privacy Protection Rule)
NERC CIP Standards - (NERC Critical Infrastructure Protection Standards)
Copyright, Designs & Patents Act
Computer Misuse Act

b. MWI will comply with other laws and legislation as appropriate.

## 4 Risk Assessment and audit

4.1 MWI is responsible for ensuring that appropriate risk assessment(s) are carried out in relation to all the business processes covered by this policy. The risk assessment will identify the appropriate countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.
4.2 Storing Customers information requires MWI to undertake a self-assessment audit based on defined indicators.
4.3 Internal Audit can undertake an audit of compliance with policy on request.

## 5 Physical & Environmental Security

5.1 Core network equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that has a monitored temperature and backup power supply.
5.2 Core network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
5.3 Combination lock codes will be changed periodically, following a compromise of the code or a suspected compromise.
5.4 Critical or sensitive network equipment will be protected from power supply failures.
5.5 Critical or sensitive network equipment will be protected by fire suppression systems.
5.6 Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
5.7 All visitors to secure network areas must be authorised by a senior member of the technical support team.
5.8 All visitors to secure network areas must be made aware of security requirements.
5.9 All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.
5.10 MWI will ensure that all relevant staff are made aware of procedures for visitors.
5.11 Entry to secure areas containing critical or sensitive network equipment will be restricted to those whose job requires it. MWI will maintain and periodically review a list of those with unsupervised access.

## 6 Access Control to the Network for Employees

6.1 Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access will be via secure two-part authentication.
6.2 There must be a formal, documented employee registration and de-registration procedure for access to the network. Separate authorisation will be required for Remote Access to the network.
6.3 The CEO of MWI must approve employee access prior to any systems.
6.4 Security privileges (network administrator rights) to the network will be allocated on the requirements of the employee's job, rather than on a status basis.
6.5 All authorised employees to the network will have their own individual password.
6.6 Employees are responsible for ensuring their password is kept secret (see Customers Responsibilities 24.3).
6.7 Employee access rights will, upon notification from departmental managers, be immediately removed or reviewed for those employees who have left MWI or changed jobs.

## 7 Remote Access

7.1 Remote Access refers to any technology that enables MWI employees in geographically dispersed locations to connect to internal office or network.
7.2 MWI is responsible for ensuring that a formal risk assessment is conducted to assess risks and identify controls needed to reduce risks to an acceptable level.
7.3 MWI is responsible for providing clear authorisation mechanisms for all remote access employees.
7.4 Departmental Managers are responsible for the authorisation of all applications for remote access and for ensuring that appropriate awareness of risks are understood by proposed employees.

7.5 All remote access employees are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources and notify MWI immediately of any security incidents and/or breaches.
7.6 MWI is responsible for ensuring that the Remote Access infrastructure is periodically reviewed, which could include but is not limited to independent third party penetration testing.

## 8 Wireless Network

8.1 MWI has deployed a wireless network across many premises which is for the use of employees and authorised representatives only, to connect customers to services.
8.2 The wireless network security standards are as follows:
a) Access Layer: Customers will connect to the WLAN via Access Points, which will provide the 802.11a/b/g/n connection standard for the client devices.
b) Service Set Identifier (SSID2): The SSID for the staff access may be hidden and not broadcast thus reducing the potential for inappropriate access.
c) The SSID for 'guest' access to the Internet only, will be broadcast so as to make it easily available to authorised visitors. Access will be granted via the IT Service Desk.
d) Encryption: The wireless networks will utilise AES (Advanced Encryption Standard) level of encryption. This encryption standard is mandatory to enable the 802.11n network to be supported.
e) Authentication: The authentication protocol selected used is Protected EAP (PEAP). PEAP is an 802.1X authentication type for wireless networks.
f) The radios used by MWI staff will confirm to the WPA 2 (Wi-Fi Protected Access) standard or higher.
g) Unauthorised devices connected to the wireless network shall be blocked with no warning.
h) Staff should not attempt to connect personally owned wireless devices to MWI wireless network.

## 9 Third Party Access Control to the Network

9.1 Third party access to the network will be based on a formal contract that satisfies all necessary MWI security conditions.
9.2 The support team is responsible for ensuring all third party access to the network is logged.
9.3 No third party shall access any portion of the MWI network without written authorization from the CEO of MWI.

## 10 External Network Connections

10.1 MWI is responsible for ensuring that all connections to external networks and systems conform to the Code of Compliance and supporting guidance found in the Information Governance Toolkit.
10.2 MWI is responsible for ensuring all connections to external networks and systems are documented and approved by MWI before they commence operation.

## 11 Maintenance Contracts

11.1 MWI will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

## 12 Data and Software Exchange

12.1 Formal agreements for the exchange of data and software between organisations must be approved by MWI CEO.

## 13 Fault Logging

13.1 The Service Desk is responsible for ensuring that a log of all faults on the network is maintained and reviewed.

## 14 Data Backup and Restoration

14.1 MWI is responsible for ensuring that backup copies of network configuration and data stored on the network are taken regularly.
14.2 A log should be maintained of switch configuration and data backups detailing the date of backup and whether the backup was successful.
14.3 Documented procedures for the backup process will be produced and communicated to all relevant staff.
14.4 Documented procedures for the storage of backup tapes will be produced and communicated to all relevant staff.
14.5 All backup data will be stored securely and a copy will be stored off-site.
14.6 Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
14.7 Patches and any fixes will only be applied by MWI following suitable change control procedure.

## 15 Malicious Software

15.1 MWI must ensure that measures are in place to detect and protect the network from viruses and other malicious software.

## 16 Unauthorised software

16.1 Use of any non-standard software on MWI equipment must be approved by support team and/or MWI CEO before installation. All software used on MWI equipment must have a valid licence agreement - it is the responsibility of the MWI to ensure that this is the case.

## 17 Secure Disposal or Re-use of Equipment

17.1 MWI must ensure that where equipment is being disposed of all data on the equipment (e.g. on hard disks or other) is physically destroyed prior to leaving MWI premises for disposal.
17.2 MWI must ensure that where electronic media are to be removed from the premises for repair, where possible, the data is securely overwritten.

## 18 System Change Control

18.1 MWI is responsible for ensuring that appropriate change management processes are in place to

review changes to the network; which would include acceptance testing and authorisation. MWI is responsible for ensuring all relevant Network documentation is up to date.

18.2 MWI is responsible for ensuring that selected hardware or software meets agreed security standards.

18.3 Testing facilities will be used for all new network systems. Development and operational facilities should be separated.

## 19 Security Monitoring

19.1 MWI is responsible for ensuring that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

19.2 MWI reserves the right to access, modify or delete all data stored on or transmitted across its network. This includes data stored in personal network folders, mailboxes etc. Data of a personal nature should be stored in a folder marked or called 'Private'. This does not preclude access or removal of such a folder on the authority of a senior support or MWI CEO.

19.3 MWI reserves the right to disconnect or block any device connected either by physical or wireless means to the network.

19.4 MWI reserves the right to block any physical non-approved device connected to a piece of MWI owned equipment.

## 20 Training and Awareness

20.1 MWI CEO and support team will work in conjunction with technical staff and non-technical employees to provide security awareness training for all staff to ensure that they are aware of their responsibilities for security, and the actions that they need to undertake in order to discharge those responsibilities.

20.2 All employees of MWI must be made aware of the contents and implications of the Network Security Policy.

## 21 Reporting Data Security Breaches and Weaknesses

21.1 Data Security Breaches and weaknesses, such as the loss of data or the theft of a laptop, must be reported in accordance with the requirements of MWI's incident reporting procedure and, where necessary, investigated by the support team.

## 22 System Configuration Management

22.1 MWI will ensure that there is an effective configuration management process for the network.

## 23 Disaster Recovery Plans

23.1 MWI will ensure that disaster recovery plans are produced for the network and that these are tested on a regular basis.

## 24 Unattended Equipment and Clear Screen

24.1 Customers must ensure that they protect the network from unauthorised access. They must log off the network when finished working.
24.2 MWI operates a clear screen policy that means that Customers must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked or a screensaver password activated if a workstation is left unattended for a short time.
24.3 Customers of dumb terminals must log out when not using the terminal.

## 25 Responsibilities

### 25.1 Support Team Responsibilities

25.1.1 Act as a central point of contact on network security within the organisation, for both staff and external organisations.
25.1.2 Implement an effective framework for the management of network security.
25.1.3 Assist in the formulation of Network Security Policy and related policies and procedures.
25.1.4 Advise on the content and implementation of the relevant action plans.
25.1.5 Produce organisational standards, procedures, and guidance on Network Security matters for approval by MWI. All such documentation will be included in the Asset register.
25.1.6 Co-ordinate network security activities particularly those related to shared information systems or IT infrastructures.
25.1.7 Liaise with external organisations on network security matters, including representing the organisation on cross-community committees.
25.1.8 Create, maintain, and give guidance on and oversee the implementation of network security.
25.1.9 Represent the organisation on internal and external committees that relate to network security.
25.1.10 Ensure that risks to network systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
25.1.11 Ensure the systems, application and/or development of required policy standards and procedures in accordance with business needs, policy and guidance.
25.1.12 Ensure that access to the organisation's network is limited to those who have the necessary authority and clearance.
25.1.13 Provide advice and guidance to development teams to ensure that the policy is complied with.
25.1.14 Approve system security policies for the infrastructure and common services.
25.1.15 Approve tested systems and agree plans for implementation.
25.1.16 Advise on the accreditation of IT systems, applications and networks
25.1.17 Ensure that Network Security is included within MWI Mandatory training programme.
25.1.18 Support incident assessments, where necessary
25.1.19 Provide support on Customers matters relating to Network Security
25.1.20 Ensure the security of the network, (that is information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements and obligations.
25.1.21 Ensure that staff are aware of their security responsibilities.
25.1.22 Ensure that staff have had suitable security training.
25.1.23 Ensure that the support team is promptly notified when new accounts are required.
25.1.24 Ensure that the support team is promptly notified when existing accounts are to be reviewed or deleted, e.g. when a member of staff changes roles or leaves the organisation.

### 25.2 Employee Responsibilities

All personnel or agents acting for the organisation have a duty to:

25.2.1 Safeguard hardware, software and information in their care.
25.2.2 Prevent the introduction of malicious software on the organisation's IT systems.
25.2.3 Customers are responsible for ensuring their password is kept secret - ***passwords should not be shared under any circumstances.***
25.2.4 Passwords should be changed regularly and be such that they are not easily guessed e.g. names of relatives or pets. Network passwords must:

a) be changed every 30 days
b) not contain the employee network account name or parts of the employee full name that exceed two consecutive characters
c) be at least 8 characters in length
d) contain characters from three of the following four categories:
i. English uppercase characters (A through Z)
ii. English lowercase characters (a through z)
iii. base 10 digits (0 through 9)
iv. non-alphabetic characters (for example, !, $, #, %)

25.2.5 If a Customers suspects that their network password has become compromised, they should report this to the IT Service Desk and change their password.
25.2.6 Report on any suspected or actual breaches in security.

## 26 Development of Procedural Document

26.1 Prioritisation of work

This document has been developed so that all employees are aware of the associated information technology requirements within the organisation in a consistent manner, ensuring that new employees are practicing in a way that ensures best practice.

26.2 Consultation and Communication with Stakeholders

This policy and subsequent programme was developed in consultation with a number of staff focus groups and in conjunction with as well as MWI partners who share a common local area network infrastructure.

26.3 Approval of policy

- The director lead for this policy is the CEO of MWI, the responsibility for the development has been delegated to the support team.
- The MWI CEO is responsible for the final approval of this policy