1.0 Objective

The purpose of these policy is to ensure that security of information and systems, accessed through teleworking and mobile devices are given due importance. It is essential that Infinit-O team members have the knowledge that security procedures and policies exist and they are understood and adhered to.

2.0 Scope

This policy and procedures includes all Infinit-o persons/parties who have access to company information and company systems belonging to or under control of Infinit-O.

3.0 Responsibilities

EXECOM are responsible for ensuring that all staff and managers are aware of security policies and that they are observed. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems. Designated owners of systems, who have responsibility for the management of information and communication technology systems and information, need to ensure that staff are aware of their responsibilities towards security. Designated owners of systems and information need to ensure they uphold the security policies and procedures.

4.0 Provisions

4.1 For teleworking and mobile working, access to Infinit-O information and applications (including email) can be attained via use of Infinit-O commissioned devices. This is composed but not limited to Computers, Laptops, Mobile Devices, Tablets

4.2 Team members entrusted with a company laptops and mobile devices are responsible for ensuring that it is regularly connected to the company network for automatic upgrade of anti-virus software and other software.

4.3 Mobile devices distributed by the Company should only be used by authorized parties in accordance with the Company Acceptable Use Policy and associated security policies.

4.4 All users accessing Infinit-O resources via teleworking and mobile devices (company owned or not) must abide by the company security policies.

4.5 Active equipment that is unlocked and in use should not be left unattended at any time.

4.6 A password should be set up and used on all equipment that can be locked by use of a password. For example, ipad devices can be set locked using a password and this facility should not be disabled by the user.

4.7 Users must not alter or disable any element of the configuration of devices, including data encryption and anti-virus software

4.8 Connection to the Infinit-O's network should only be attempted using the credentials which team members are issued with. Connection using network infrastructure that does not belong to the Company may enable traffic to be viewed, altered or deleted by an attacker

4.9 Users conducting teleworking/mobile working should not allow or give permission for unauthorised users (including family and friends) to use that PC/mobile device.

4.10 Any information concerning passwords, usernames, network credentials or requirements/ability used to access the Company information and systems by teleworking/mobile working must not be shared with other team members, unauthorised users, third party vendors, family, friends or members of the public

4.11 During short periods of time when devices are not being used (e.g. when on the phone) users must lock PCs and devices to prevent screens being overlooked. For example, on PCs/laptops this can normally be achieved by holding down the ctrl-alt-del keys together and choosing the 'lock computer' option or by holding down the Windows (flag) key and hitting the L key.

4.12 Users should ensure that all applications are properly closed/logged off, browsers are closed and internet sessions are logged off, prior to network connections being logged off and closed.

4.13 On completion of work, teleworkers/mobile workers should fully power down or log off remote devices like laptops and thin clients. Devices should not be suspended but fully powered down.

4.14 Transfer of personal or restricted information must take place through a secure, encrypted channel (identified by the https address prefix and padlock symbol) using suitable software/applications.

4.15 Person identifiable information and/or business data should not be stored on the PC/mobile device. If possible data should be accessed from and be stored on company servers or on password protected and encrypted portable/removable media.

4.16 Person identifiable information and data should only be sent using official channels, authorised software/applications and official equipment deemed fit for the purpose. For example, messages containing person identifiable information and data should not be sent via SMS/TXT.

4.17 Users should always be aware of the potential for other people (including family, friends, colleagues and intruders) to overlook screens and keyboards and view personal, confidential information or passwords. Users should check that this is not taking place during processing of data.

4.18 It is possible to access Infinit-O email from a remote location (such as home) using non-wireless or wireless technology. This should only be attempted using a web browser via https://mail.google.com . Team members must ensure when using this service that https is displayed at the start of the address line and the padlock symbol is displayed on the browser window. At the end of using this email service staff must logoff webmail and close the browser window. Failure to do so can leave the account accessible to hackers.

4.19 Extra care should be taken to properly close all applications, network connections and web browsers when using PCs, mobile devices and software not officially provided by the company. Passwords, logon credentials and sensitive files can be left behind on un-trusted devices, making them readily available to subsequent users.

4.20 Team members should only use a home Wi-Fi system as a last resort but if this becomes necessary they must ensure that the network is a secure as possible. Team members must connect via Wi-Fi through WPA2 standard (as minimum) and that they adhere to the Infinit-O password provisions. (See accompanying information concerning 'Wi-Fi security' at the end of this policy)

4.21 In the event that a user becomes aware of an information or data breach or accidental disclosure, this matter must be reported immediately via the Company Incident Reporting Procedures (QMMS).

5.0 References

This document has been prepared using the following ISO270001 standard control as reference

ISO Control	Description
A.6.2	Mobile devices and teleworking
A.11.1.5	Working in secure areas
A.11.2.1	Equipment siting and protection
A.11.2.6	Security of equipment and assets off-premises
A.11.2.8	Unattended user equipment
A.13.2.1	Information transfer policies and procedures
A.12.6.2	Restrictions on software installation
A.11.2.9	Clear desk and clear screen policy

6.0 Version History

VERSION	DATE	DETAIL	AUTHOR
1.0	**09/21/15**	**Completed for distribution**	**Wilmar Cundangan**
1.0	**09/22/15**	**Approved by ISO Group**	**Wilmar Cundangan**

Wi-Fi Security.
Computers and many other devices, including smart phones and PDAs, can connect to the internet wirelessly using Wi-Fi. An unsecured Wi-Fi connection makes it easier for hackers to access private files and information and it allows strangers to use the internet connection for their own purposes.

These are general tips on changing private router and network settings. Team members may need to check the instructions for their wireless equipment for the technical details. If staff need more guidance on checking or changing settings, the Wi-Fi equipment supplier or internet provider will provide advice on their websites.

How do I check whether my network is secure?
Wi-Fi networks are accessed through a physical device called a router – also known as a hub. Staff will need to connect to their router to check its network settings. To do this, staff will need the router's IP address, user name and password. Open the browser and enter the router's IP address into the address bar. When asked, enter username and password. The router settings will allow staff to find out whether the connection is already secured and will let a more secure password be chosen.

How do I secure my network?
The following tips will help team members to use Wi-Fi more securely and to protect personal information.

Change the wireless network's default name
A Service Set Identifier (SSID) is a unique ID used for naming wireless networks and ensures the network name is different to other nearby networks. Team members should change the network name

from the router's default. This will make it harder for anyone to identify the browser and guess its default settings.

Use encryption
Encryption scrambles messages sent over wireless networks so that they cannot be read easily. If the network is not encrypted, then staff should enable encryption on their settings page. There are different forms of encryption, but the Company requires that staff use the Wi-Fi Protected Access (WPA/WPA2) version because it is stronger than other versions such as Wired Equivalent Privacy (WEP).

Choose a strong password
Change the password from a default supplied with the router. Make sure the password is easy to remember but would be difficult for a stranger to guess and preferably something with a combination of letters and numbers. Avoid using something obvious such as street name.

Check that the device does not auto-connect to Wi-Fi signals
If the device is set to automatically connect to available Wi-Fi networks, then team member run the risk of automatically connecting to unknown and potentially dangerous networks. Team members should switch off auto-connect on the device settings page – refer to the manufacturer's instructions for more details.