REMOTE ACCESS & MOBILE COMPUTING POLICY

Introduction

This Policy addresses the risks to the Organisation's information systems posed by mobile computing and by access to its network by outside parties. Mobile computing equipment can relatively easily fall into the wrong hands. Remote connectivity can open routes into sensitive Organisation systems and information for hackers or malicious codes of all kinds. The Organisation takes these risks very seriously.

Responsibilities

Senior Management are responsible for ensuring that this Policy is complied with.

All of the Organisation's employees are responsible for maintaining remote access and mobile computing security in accordance with this Policy.

Remote Access: General

All employees of the Organisation have been instructed as follows irrespective of the mode of remote access:

1. Logins and passwords must not be revealed to anyone, including family members
2. The Organisation's Password Policy applies to remote access usage. Strong passwords (see Password Policy) must be used at all times
3. Once logged in, the connection is never to be left unattended
4. Access to the Organisation's IT systems is for the authorised user only. Under no circumstances is any other party to be allowed to make use of such access
5. When connected via remote access to the Organisation's IT systems, users must not be connected to any other network of any kind unless previously authorised by the Internal IT Manager
6. Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual-homing is not permitted at any time unless previously authorised by the Internal IT Manager
7. Any devices that are used to access the Organisation's networks must be protected by a firewall. Personal PCs or laptops must be cleared for such use by the Internal IT Manager before their use
8. No user's personal PC or laptop should have any Organisation documents or files of any kind stored on its hard disk unless specifically authorised by the Internal IT Manager. If authorised to work from home, the user may download documents to work on them but must ensure security and integrity of those documents
9. The Organisation's E-mail & Internet Acceptable Usage Policy applies to all remote users, irrespective of the means by which they access the Organisation's systems

Anyone who suspects that there may have been a breach of network security via remote access must report it immediately to the Internal IT Manager.

Mobile Computing Facilities

The following applies to all users of IT equipment, software and services provided by the Organisation for use outside of the Organisation's offices. These are called 'mobile computing facilities' in the following and can include laptops, PDAs, PCs set up in employees' homes, etc.

All employees of the Organisation have been made aware of the following rules, requirements and guidelines:

1. Mobile computing with remote access is meant to be an alternative or additional method of meeting the Organisation's requirements. The Organisation may terminate such an arrangement at any time
2. Mobile computing facilities provided by the Organisation are to be used only for creating, researching and processing Organisation-related materials. By using such facilities the user assumes personal responsibility for their appropriate use and agrees to comply with all of the applicable Organisation's Policies, rules, requirements and guidelines as well as all relevant statutory, regulatory and similar requirements
3. Hard disks and other storage media are subject to audit without notice, in order to ensure compliance with all of the applicable Organisation's Policies, rules, requirements and guidelines as well as all relevant statutory, regulatory and similar requirements
4. This equipment must be protected with a strong password at BIOS or hard disk level so that no unauthorised user can work with it or access the information on the hard disk or other storage. This is in addition to any network login and password if applicable
5. This equipment must never be left powered up and unattended. For added security, all information on screen should be protected by either power management or a password protected screensaver
6. Users of mobile computing facilities are responsible for the contents of hard disks and other storage. If it is necessary to send a unit away for repair, the user must liaise with the Internal IT Manager to ensure that any sensitive information is erased beforehand.

Users of mobile computing facilities, particularly but not exclusively laptops, must exercise extreme care that the unit does not leave their control by means of loan, theft or any other circumstances. Loss or theft must be reported immediately to the police, to the ISMS Manager or a Director.

General

This Policy specifically applies to employees with remote access rights to the Organisation's network systems.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	15/10/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Update of responsibilities and dates