1 User Details

Name: _____

Position: _____

Department: _____

User access request originated by: _____

User access request approved by: _____

User access request processed by: _____

User access account username allocated: _____

Email address allocated: _____

Signed and agreed by staff member present: _____

User signature of acceptance of access rights and responsibilities as set out in this agreement: _____

1.1 I accept that I have been granted the access rights defined in this agreement to those organisational information assets (including laptop, workstation, tablet, mobile phone etc) also identified in this agreement.

1.2 I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions.

1.3 I accept and will abide by the company's Acceptable Use of Assets Policy (DOC A8.3).

1.4 I will immediately report information security incidents and weaknesses that I observe or become aware of to the IT Service Desk.

1.5 I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the company's disciplinary policy.

1.6 I acknowledge that I have received adequate training in relevant aspects of my use of company systems and of my responsibilities under this agreement.

2 Passwords

2.1 I will select and use passwords that comply with the company Password Policy (DOC A9.3).

2.2 I will change my initial temporary password at first logon.

2.3 I will keep my passwords secret and will not under any conditions divulge them to or share them with anyone, except known members of the IT Department for support purposes.

2.4 I will not write down passwords where others can view or access them, nor record them anywhere without having obtained the specific authorisation.

2.5 I will change my password at intervals as required by the company, will not attempt to re-use passwords or use new passwords that are in a sequence, and will change my password immediately if there is evidence or concern of possible system or password compromise.

2.6 I will not store my password in any automated logon process, unless instructed to do so by a member of the IT department.

2.7 I will not use the same password for organisational and personal use.

3 Multi Factory Authentication (MFA)

3.1 I will setup MFA on all my accounts where available or instructed to do so before attempting to access any company data or systems.

4 Clear Desk Policy, Screen Savers and Information Reproduction

4.1 I understand that I am required to ensure that no confidential or restricted information (in paper or removable storage media format) is left where it may be compromised when I am not in attendance and will ensure that such information is secured in line with company security requirements.

4.2 I understand that I am required to ensure that no one is able to access my information assets (including laptop, workstation, tablet, mobile phone etc) when I am not in attendance and that I must have a password protected screensaver that operates as per company standards or which I activate when I leave the information assets unattended.

4.3 I know that I am required to terminate active computer sessions when I have finished with them and logoff / shutdown my device whenever I am finished working.

5 Software

5.1 I will ensure that no attempts are made to disable or over-ride any of the company's installed software, including anti-malware software, firewalls and automatic updating services.

5.2 I accept that I may not download from the Internet or install on any company computer or other device any software of any sort for which the company does not have a valid licence and that has not had the prior authorisation of the Head of IT.

5.3 I recognise that this prohibition includes freeware, shareware, screensavers, toolbars and/or any other programs that might be available.

6 Data Control and Legislation

6.1 I will obtain the written authorisation of the IT Service Desk for the storage of any personal information (mine or anyone else's) on company systems.

6.2 I will ensure that I abide by any legal requirements in respect of my computer use, including privacy and data protection regulations.

7 Maintenance

7.1 I accept that I am responsible for the physical security of my assigned information assets (including laptop, workstation, tablet, mobile phone etc) and will report any faults or issues to the IT Service Desk.

8 Revocation and change of access rights

8.1 I understand that any breach of these conditions may result in revocation and/or change of access rights.

9 Own equipment

9.1 I will comply with the company's requirements regarding the connection of my own equipment to the company's systems and when accessing any information including allowing the ability to remote access a device where required.

9.2 Further, I shall operate any equipment and processing of information as I would if in the office (this includes not allowing others such as family or friends access to the equipment and information in any manner).

Document Control

The Security and Governance Manager is responsible for ensuring this document remains current and up to date.

A current version of this document is available to all members of staff on the company network and is published.

This policy was approved by the Head of IT and is issued on a version controlled basis.

Signature: Date:

Change History Record

Issue	Description of Change	Date of Change
1.0	Initial Issue	Dd/mm/yyyy