1. Teleworker**[[1]](#footnote-1)** name:

Position and role:

Department:

*{Manager}*:

Equipment allocated: *[attach a copy of* [*ISMS-C REC 8.1.1*](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_8.1.1.docm) *showing what equipment has been approved and who is providing it]*

Hours of access:

Access rights and classification of information to be stored: *[Insert the detailed access rights to be granted in terms of in* [*ISMS-C DOC 9*](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_9.docm)*]*

User access request originated by: *{HeadHR}*

*[Date]*

User access request approved by: *{Manager}*

*[Date]*

User access request approved by: *[Asset owner(s)]*

*[Date]*

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

Signed and agreed by staff member:

*[Date]*

User access name allocated:

E-mail address allocated:

Data storage file allocated:

User access request processed: *{ITDept}*

*[Date]*

* 1. I*, [ ],* accept that I have been granted the access rights defined in this agreement to those *{OrganisationName}* information assets also identified in this agreement, subject to the reservations of title and acceptance of liabilities set out in *[ ]* attached to this agreement. 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. I also accept and will abide by *{OrganisationName}*’s Internet Acceptable Use Policy ([ISMS-C DOC 8](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_8.docm)) and its e-mail policy (ISMS-C DOC 8).
  2. I acknowledge that I have received adequate training in all aspects of my use of *{OrganisationName}*’s systems and of my responsibilities under this agreement.

1. **Passwords**
   1. My username and password will be issued in line with *{OrganisationName}*’s procedure for authorising and issuing them.
   2. I will change my initial temporary password at first logon.
   3. I will select and use passwords that are at least 7 characters in length, are alpha-numeric, are not based on any easily guessable or memorable data such as names, dates of birth, telephone numbers etc, are not dictionary words and are free of consecutive identical all-numeric or all-alphabetic characters.
   4. I will keep my password secret and will not under any conditions divulge it to or share it with anyone, nor will I write it down and leave it anywhere that it can easily be found by someone else or record it anywhere without having obtained the specific authorisation of the *{InfoSecManager}* to do so.
   5. I will not store my password in any automated logon process.
   6. I will change my password at intervals as required by *{OrganisationName}*, will not attempt to re-use passwords or use new passwords that are in a sequence, and will change my password more frequently if there is evidence of possible system or password compromise.
   7. I will not use the same password for organisational and personal use.
   8. Replacement passwords are administered as set out in ISMS-C DOC 9; users must obtain the written permission of their *{Manager}* before a replacement password can be issued.
   9. *[Insert any additional information regarding additional authentication requirements, e.g. biometrics, tokens, etc]*.
   10. *[Insert any additional information regarding connectivity, VPNs, encryption, etc.]*
2. **Clear desk policy, screen savers and information reproduction**
   1. I understand that I am required to ensure that no confidential or restricted information (in paper or removable storage media format) is left on my desk, in my environs, or left in or near reproduction equipment (photocopiers, fax machines, scanners) when I am not in attendance and will ensure that such information is secured in line with *{OrganisationName}*’s security requirements[[2]](#footnote-2) as set out in ISMS-C DOC 8.
   2. I understand that I am required to ensure that no one is able to access my workstation when I am not in attendance and that I must have a password protected screensaver that operates within *[five]* minutes of no activity or which I activate when I leave the workstation unattended.
   3. I know that I am required to terminate active computer sessions when I have finished them and to log off (i.e. not simply turn off the computer screen) whenever I am finished working *[and that the workstation is to be protected by appropriate key locks when I am away from the building]*.
   4. I accept that I am not allowed to *[use/bring in to the office]* personal storage media, MP3 players, digital cameras and mobile phones with photographic capability.
   5. I accept that I may only use *{OrganisationName}*’s reproductive equipment (photocopiers, fax machines, scanners) for proper organisational purposes and that I will ensure that I will use facilities that are appropriate for the classification level of any information with which I am dealing.
3. **Software**
   1. I will ensure that no attempts are made to disable or over-ride any of *{OrganisationName}*’s installed software, including anti-malware software, firewalls and automatic updating services.
   2. I accept that I may not download from the Internet or install on any organisational computer or other device any software of any sort for which *{OrganisationName}* does not have a valid licence and that has not had the prior authorisation of the *{HeadIT}*. I recognise that this prohibition includes freeware, shareware, screensavers, toolbars and/or any other programs that might be available.
   3. I recognise that *{OrganisationName}*’s requirements in respect of the use of Instant Messenger facilities is *[ ]* and will abide by it.
4. **Data control and legislation**
   1. I will obtain the written authorisation of the *{DataProtectionOfficer}* for the storage of any personal information (mine or anyone else’s) on *{OrganisationName}*’s computer systems.
   2. I will ensure that I abide by any legal requirements in respect of my computer use, including privacy and data protection regulations.
5. **Backup and information classification**
   1. I acknowledge that I am responsible for ensuring that all information on my *[workstation]* is correctly classified and labeled in line with the requirements of ISMS-C DOC 8. I will ensure that this requirement is complied with.
   2. *[Insert any additional requirements regarding encryption, etc.]*
   3. I acknowledge that I am responsible for backing up information on my *[workstation]* in line with the requirements of control 8.2.2 and 8.2.3 of SoA in the [Manual](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/InfoSecManual.docm). I understand that I am required to store all data [where, how?] and that I may not store organisational information other than in line with approved organisational requirements.
6. **Maintenance, insurance and return of equipment**

*[Insert clauses setting out how equipment is to be maintained, what the revocation rights are, how you get kit back at the end of the contract/employment, how insurance is dealt with.]*

1. **Audit and security monitoring**

*[Set out here how you will handle this, noting that you will need to carry out remote monitoring, and what audits you will need to do.]*

***Document Owner and Approval***

The *{InfoSecManager}* is the owner of this user agreement template and is responsible for ensuring that it is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to *[all/specified]* members of staff on the *[corporate intranet]* and is published *[ ].*

This user agreement template was approved by the *{ChiefInfoSecOfficer}* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |

**ANNEX TO THE USER AGREEMENT**

This annex contains details of notebook configurations, service connection and backup procedures that may change from time to time.

1. This document may need to be used in a disciplinary situation, so you need to be sure that your legal advisers are happy that it conforms to your local jurisdictional requirements. The teleworker user agreement needs to be adjusted to take into account all the requirements of Clause 6.2.2 of ISO27002 and the guidance of **Chapter 21** of [IT Governance: An International Guide to Data Security and ISO27001/ISO27002](http://www.itgovernance.co.uk/shop/p-772-it-governance-an-international-guide-to-data-security-and-iso27001iso27002.aspx). [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)