1. **Scope**

All *users/user groups* that need to access {OrganisationName} information have specific, pre-determined access rights to information, operating systems and applications that conform to and are restricted by the Access Control Policy.

1. **Responsibilities**
   1. The *{HeadIT}* is responsible for creating, documenting and maintaining individual *user/user group* profiles that meet the requirements of the Access Control Policy.
   2. The *{HeadIT}* is responsible for creating, documenting and maintaining individual *user/user group* profiles that meet the requirements of the Access Control Policy. This person is also responsible for administration of allocated and authorised *user/user group* access rights in conformity with the policy.
   3. The *{HeadHR}* is responsible for initiation and administration of new and changed user access requests (user agreements) and user training.
   4. *{Manager}* are responsible for authorising access requests as being in line with business and {OrganisationName} security policy and procedure.
   5. Asset *[owners]* are responsible for authorising access requests to their information assets as being in conformity to the security requirements of the asset.
   6. The *{InfoSecManager}* is responsible for reviewing user access rights in line with the review requirements of the ISMS.
2. **Access control policy**
   1. {OrganisationName} controls access to information on the basis of business and security requirements.
   2. Access control rules and rights to applications, expressed in standard user profiles, for each *user* / *group of users* are clearly stated below, together with the business requirements met by the controls.
   3. The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.
   4. The access rights to each application take into account:
      1. The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the *[systems and]* network(s).
      2. Data protection (DPA 1998) and privacy *[and other?]* legislation and *[any?]* contractual commitments regarding access to data or services.
      3. The ‘need-to-know’ principle (i.e. access is granted at the minimum level necessary for the role).
      4. ‘Everything is generally forbidden unless expressly permitted’.
      5. Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.
   5. {OrganisationName} has standard user access profiles for common roles in {OrganisationName}.
   6. Management of access rights across the network(s) is *[done how?]*.
   7. User access requests, authorisation and administration are segregated as described below.
   8. User access requests are subject to formal authorisation, to periodic review and to removal.
3. **Access to networks and network services**
   1. Users are only provided with access to the network and network services that they have been specifically authorised to use, in accordance with [ISMS-C DOC 13](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_13.docm).
4. **User registration, de-registration and access provisioning**
   1. Every *user*’s proposed access rights are documented in a User Agreement, which details the systems/services/applications/information assets to which access is to be granted, together with the level of access that is to granted, taking into account the Access Control Policy and the standard user profiles set out below.
   2. The *{Manager}* and the system/asset *[owner*] authorise access to the system/asset.
   3. The user agreement is then signed by the *[user]* and passed to the *{HeadIT}* and the username/user ID is created and administered
   4. The *{ITDept}* maintains a list of authorised *users*, administers changes in access rights and removes users.
   5. The disciplinary policy will be invoked in cases of attempted unauthorised access.
5. **Management of privileged access rights**
   1. Privileges are allocated to a different username than that allocated for normal use.
   2. Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated in an e-mail from the *user* concerned to the *{InfoSecManager}* which sets out the reasons why the privilege is required and the *[length of time]* for which it is required.
   3. The *{InfoSecManager}* retains a log of all privileges authorised and allocated and checks on a *[state regularity]* basis that they have been de-activated as specified in the original request.
   4. The *{InfoSecManager}* checks *[how?] [on a monthly basis]* that unauthorised privileges have not been obtained.
6. **Management of secret authentication information of users**
   1. User password responsibilities are documented in their signed User Agreements.
   2. *Users* are initially *[encrypted/hashed – how? And how do users acknowledge receipt of their passwords?]* issued with a unique temporary password which they are forced to change at first logon.
   3. *[Monthly]* password changes are enforced, reuse of passwords is prohibited for 16 subsequent attempts, and seven-character alphanumeric passwords are required.
   4. Passwords are stored on *[where]*, are stored separately from application system data and are protected by [*details of access controls and encryption levels].*
   5. *[Insert any additional details that apply to two-factor authentication – biometrics, tokens, etc. – either here or referenced in work instructions.]*
   6. The default passwords on all new equipment are changed to conform with {OrganisationName}’s password requirements before the equipment is brought into service.

1. **Removal or adjustment of access rights**
   1. The access rights of all employees and contractors to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.
   2. Upon termination or change of employment, complete a termination checklist ([ISMS-C REC 7.3.1](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_7.3.1.docm)) to confirm that all access rights have been removed or adjusted.
2. **Use of secret authentication information**
   1. Users are required to follow {OrganisationName}’s practices in use of secret authentication information.
3. **Information access restriction**
   1. Access to information and application system functions by users and support personnel is restricted by the use of standard user profiles in accordance with the access control policy.

| **Classification** | **Access Rights** | **Example** |
| --- | --- | --- |
| **Guest** | Able to see and read public data.  Full create and edit rights to a private data space. | Clients |
| **Trustee** | Full rights to a shared directory or sub system.  Able to see and use basic business templates and core information sources and systems. | Partner Organisations  Software maintenance  Data input staff  Anyone who has signed a Non-Disclosure agreement |
| **Individual** | Full private access to a secure private drive.  Able to create files in a user group and delete owned files in that user group.  Able to grant access rights to ‘Private’ files or directories to others.  Access rights to restricted and confidential information dependent on role requirements. | Jsmith@organisation.co.uk |
| **Supervisor** | Full unrestricted rights to create new users and configure PC’s and create user groups and manage the network. | IT staff |
| **Administrator** | Full unrestricted rights to defined systems and the ability to create and remove system supervisors. | *{ITDept}*  *{ChiefExecutiveOfficer}* has right to read and edit all confidential/restricted documents |

1. **Secure log-on procedures**
   1. The screen displays no system or application identifiers until the logon has been successfully completed.
   2. The display on the logon screen includes a standard notice *[detail your precise warning that the computer should only be accessed by authorised users, with a brief description of the criteria by which they are identified (e.g. [employees/staff] of {OrganisationName})]*
   3. The screen provides no help messages during the logon procedure.
   4. The system validates the logon data only on completion of input and then, if there is an error, the system requires the [*user*] to try again.
   5. The logon procedure limits the number of unsuccessful attempts allowed to three (and unsuccessful attempts are automatically recorded) and *[automatically either enforces a time delay before further attempts are allowed, or simultaneously disconnects the data link, sends an alarm and rejects any further attempts without specific authorisation from the {SystemAdmin}, the user having first been positively identified by the {SystemAdmin}]*.
   6. The system limits the maximum time allowed for the logon attempt to *[minutes]* and, when the limit is exceeded, the system terminates logon.
   7. Password characters are hidden by symbols and always encrypted *[how?]* before being sent across the network.
2. **Use of privileged utility programs**
   1. *[You need to decide how you want to tackle system utilities in the light of Clause 9.4.4 of ISO27002. Your options will be very much a function of the size and complexity of your organisation, the way in which you need to distribute the use of system utilities, your applications and operating systems, etc. Once you have decided what you want to do (in the light of your risk assessment), you can set out the procedure for how you do it. Remember to link this procedure in with* [*ISMS-C DOC 8*](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_8.docm) *(classification levels), and user access rights and user registration above so that you have a set of integrated procedures.]*
3. **Access control to program source code**
   1. The *{ChangeManager}* securely stores removable media and system documentation *[need to specify precisely how this is done and recorded]* and maintains a secure program list and access control list in which each application *[owner]* specifies who is authorised to access the related system documentation and program source libraries *[identify the secure area where this is all held]*.
   2. *ISMS DOC [ ]* sets out procedures for the management and maintenance of program source code and program source libraries, including how updates and issues of program sources, and copying of program source libraries, are authorised.
   3. An audit log is maintained of all access to program source libraries *[specify where and how]*.

***Document Owner and Approval***

The *{InfoSecManager}* is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

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

This policy was approved by the *{BoardDirectors}* on *[date]* and is issued on a version controlled basis under the signature of the *{ChiefExecutiveOfficer}*.

Signature: Date:

**Change History Record**

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