

User Access Management Procedure

Reference: CES DOC 3.3

DocumentKits Issue No: 1.0

Organisation Issue No:

DocumentKits Issue Date: 20/05/2020

Organisation Issue Date:

1. Scope

The access rights of all

"users/user groups"

(as specified in the [Access Control Rules and Rights Procedure \(CES DOC 3.2\)](#)) to any of Organisation Name's information assets, systems or services are managed in accordance with this procedure. Organisation Name operates "a single sign-on process."

2. Responsibilities

2.1 The Head of IT (CIO) is responsible for administration of allocated and authorised "user/user group"

access rights in conformity with the policy.

2.2 The Head of HR is responsible for initiation and administration of new and changed user access requests (user agreements) and user training.

2.3 The Manager/Executive (genericline) are responsible for authorising access requests as being in line with business and organisational security policy and procedure.

<<2.4-2.5 removed for sample purposes>>

3. User registration and de-registration

3.1 User agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access. Organisation Name's standard user agreement template is [CES DOC 3.4](#).

3.2 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 be granted, taking into account

the [Access Control Policy \(CES DOC 3.1\)](#) and the standard user profiles set out in the [Access Control Rules and Rights Procedure \(CES DOC 3.2\)](#). If a user is to be granted access rights other than the standard ones set out in the [Access Control Rules and Rights Procedure \(CES DOC 3.2\)](#), then the specific additional authorisation of the Information Security Manager is also required.

3.3 The Manager/Executive (genericline) and the
"system/asset Owners"

authorise access to the
"system/asset."

<<3.4-3.6 removed for sample purposes>>

4. Privilege management

4.1 Privileges are allocated to a different username than that allocated for normal use.

4.2 The available access privileges for each of Organisation Name's operating systems, applications and other systems, are identified and documented in the [Access Control Rules and Rights Procedure \(CES DOC 3.2\)](#).

4.3 Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated in an email from the Users concerned to the Information Security Manager, which sets out the reasons why the privilege is required and the
"length of time"

for which it is required.

<<4.4-4.5 removed for sample purposes>>

5. Password policy

5.1 The allocation of passwords is formally controlled.

""

5.2 User password responsibilities are documented in their signed user agreements.

<<5.3 removed for sample purposes>>

5.4

"Monthly password changes are enforced, re-use of passwords is prohibited for 16 subsequent attempts, and passwords must meet the following requirements:"

5.4.1 A minimum of eight characters in length

5.4.2 Differs from the associated username

5.4.3 Contains no more than two identical characters in a row

5.4.4 Is not a dictionary word

5.4.5 Includes both numeric and alphabetic characters

5.5 Users must not use the same password elsewhere, either for work or at home.

<<5.6-5.12 removed for sample purposes>>

6. Review of user access rights

6.1 Access rights are reviewed

"insert regularity"

and their adequacy is confirmed; any changes that need to take place are actioned in line with the [Username Administration Work Instruction \(CES DOC 3.3A\)](#).

6.2 User access rights are reviewed when a User's role or location within Organisation Name changes in any way. If the access rights need to change, a new user agreement is issued, in line with this procedure, setting out those access rights.

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).