Data Safe Haven Access Control Policy

1. Document Information	
Document Name	UCL-IG36 Data Safe Haven Access Control Policy
Author	Jack Hindley
Issue Date	06/07/2021
Approved by	Senior Information Risk Owner
Next review	Three years

2. Document History		
Version	**Date**	**Summary of change**
0.1		First draft for discussion
0.5	23/11/2017	Incorporated comments from Data Safe Haven Operational Management group
1.0	27/11/2017	Approved by Chair of IG Steering Group
1.1	31/01/2020	Amended to ensure user access is reviewed by information asset owners, user responsibilities now include up to date training and added glossary; also minor clarifications of terminology
2.0	06/02/2020	Approved by IG Steering Group
2.1	23/06/2021	Added statement on confidentiality in contracts
3.0	24/06/2021	Approved by Senior Information Risk Owner

1 Purpose

The purpose of this Access Control Policy ('the policy') is to ensure a consistent approach to security in access control to information assets wherein access to confidential information is provided strictly on a 'Need to Know' basis.

2 Scope

The policy applies to all users of the UCL Data Safe Haven.

Terminology

Term	*Meaning/Application*
SHALL	*This term is used to state a **Mandatory** requirement of this policy*
SHOULD	*This term is used to state a **Recommended** requirement of this policy*
MAY	*This term is used to state an **Optional** requirement*

Policy

General

- *Access **shall** be granted using the principle of '**Least Privilege'**. This means that every program and every user of the system **should** operate using the least set of privileges necessary to complete the job.*
- *UCL staff members are bound by contract of employment to maintain confidentiality. Non-staff users **shall** be bound by contracts specific to each study or user, which **shall** include a confidentiality clause.*
- *Each user **shall** be identified by a unique user identity so that users can be linked to and made responsible for their actions.*
- *The use of group identities **shall** only be permitted where they are suitable for the work carried out (e.g. training accounts or service accounts).*
- *During their induction to the system each user **should** be given a copy of guidelines for staff on use of the system and their user login details, and **should** be required to sign to indicate that they understand the conditions of access.*
- *Records of user access **may** be used to provide evidence for security incident investigations.*

Physical Access

- *Physical Access **shall** only be granted on the authority of the Service Owner and **shall** be applied on a strict 'Need to Know' basis.*
- *All Data/Systems **shall** be physically protected in accordance with their value and Classification according to the Information Management Policy.*
- *Information Asset Owners **shall** implement physical security measures in order to control Physical Access to their data/systems, in addition to any physical access controls for the buildings in which they are located.*
- *The Service Owner **should** retain a log 'date/time/name/reason' for access to their data/system.*

- *Any unauthorised access **shall** be reported as an Information Security Incident.*

Network Access

- *All staff and contractors who access the Data Safe Haven networks remotely **shall** only be authenticated using the approved remote access authentication mechanism.*
- *Diagnostic and configuration ports **shall** only be enabled for specified business reasons. All other ports **shall** be disabled or removed.*
- *Risk assessments **shall** be conducted by the Data Safe Haven Operational Management Group to determine the requirements for the segregation of networks.*
- *Segregation of networks **shall** be implemented as determined by the results of the risk assessment.*
- *Network administrators **shall** group together information services, users and information systems as appropriate to achieve the required segregation on networks.*
- *Network routing controls **shall** be implemented to support the access control policy.*

Operating System Access

User Responsibilities

- *All Data Safe Haven users **shall** be expected to confirm they are an authorised user at log-on.*
- *All Data Safe Haven users **shall** be required to change their passwords at frequent intervals and in accordance with the password management policy.*

System Configuration

- *Only authorised personnel **shall** have access to system utilities and access **should** be revoked when there is no longer a business reason for access.*
- *Where there is a business requirement for the use of identifiers that are not associated with a single individual (for example, service accounts), these **shall** only be created following consultation with the relevant service operational manager.*
- *All user sessions **shall** be configured to lock automatically after a period of inactivity in order to reduce the risk of unauthorised access.*
- *Restrictions on connection times to sensitive systems **should** be considered to reduce the window of opportunity for unauthorised access.*

Information System Access

User Responsibilities

- *All users **shall** ensure that they lock their screens whenever they leave their desks to reduce the risk of unauthorised access.*
- *All users **shall** keep their passwords confidential.*
- *Passwords **shall** be changed at regular intervals and this **shall** be enforced by the system.*
- *Passwords **shall** be changed whenever there is an indication of possible system compromise.*
- *Dual-factor login tokens shall be kept physically secure by the user and theft/loss of these shall be reported to an administrator immediately.*

- *Users **shall** maintain a record of the required data security training as per the Training Policy and **shall** make this available to the Service Owner when requested.*

Administration

- *Access to information systems shall be granted using a formal user registration process.*
- *Managers **shall** review user access rights on a regular basis and after any changes to user roles and responsibilities.*
- *Each user of a system **shall** have a unique user identity, so that the user can be held accountable for any actions carried out by their allocated user identity.*
- *A formal record of all users connected to the Data Safe Haven system **shall** be maintained, including the necessary approvals.*
- *Privilege access management **shall** be controlled through a formal process and only the minimum privileges **shall** be granted to carry out the role or task.*
- *A formal record of all privileges allocated **shall** be maintained.*
- *When a user account is no longer required, e.g. through staff resignation or a change in duties the account **shall** be disabled immediately on notification.*
- *Unused accounts **shall** be monitored and appropriate action taken in line with Data Safe Haven procedures for disabling and deleting accounts.*
- *Information asset owners **shall** acknowledge and adjust current user access regularly to reduce the risk of access persisting longer than is required*
- *Where adequate assurance is absent, account access **shall** be disabled such that re-enablement **shall** only follow evidence of adequate assurance and **shall** require formal registration*
- *Removal of accounts **shall** also include the removal of any associated access rights.*

System Configuration

- *For audit purposes, systems shall be configured to capture the unique user identity being used.*
- *Where technically possible, all standard accounts that are delivered with operating systems **shall** be disabled, deleted or have their 'default' passwords changed on system installation.*

Application and Information Access

- *All Data Safe Haven staff and contractors **shall** only be granted access to those application functions required to carry out their roles.*
- *All Data Safe Haven staff and contractors **shall** only have access to sensitive systems if there is a business need to do so and they have successfully completed any additional necessary on boarding processes as required by the relevant information asset owner.*
- *Sensitive systems **should** be physically or logically isolated in order to meet the requirements of restricted access to authorised personnel.*

Conventions used in this document

UCL policies currently employ different terminology to the DSP Toolkit. The following terms are equivalent:

DSP Toolkit and this policy	***UCL policies***
Information Asset Owner	*Data Owner*
Information Asset Administrator	*Data Custodian*

*The above are included in the more general class of **Data User**, used within UCL policies.*

UCL's glossary of terms:

https://www.ucl.ac.uk/information-security/sites/information-security/files/glossary.pdf

---