# UK LINK MANUAL

# SECURITY OPERATING FRAMEWORK

## June 2017

## Version 1 For Approval

**Version Control**

| Version | COR | Date of Change | Changes | Author |
|---|---|---|---|---|
| 1 FA | - | June 2017 | Update to reflect implementation of UNC Modification 0565A. | Rachel Hinsley |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

[STANDARD FRONT END TO BE REVIEWED]

# 1 General

## 1.1 Introduction

**1.1.1** This operating framework (**Operating Framework**) is part of the UK Link Manual referred to in GT D5 and Clause 6 of the DSC Terms and Conditions and is a CDSP Service Document.

**1.1.2** This Operating Framework is the document referred to as Annex C.1. in the UK Link Framework Document.

**1.1.3** This Operating Framework is an integral part of and is incorporated in the DSC.

**1.1.4** This Operating Framework combines the functions of a security policy and a security manual applicable to UK Link.

**1.1.5** The version of this Operating Framework which is in force, and the date from which it is in force, is as stated above.

**1.2** This Operating Framework may be changed in accordance with the applicable procedures contained in the Change Management Procedures.

## 1.3 Interpretation

**1.3.1** **"UK Link User"** has the meaning set out in GTD 5.1.2;

Some definitions used within UK Link Gemini are specific to that system but there are equivalent terms which are used in the UK Link Manual including this Operating Framework. The following shows how these terms relate to each other.

**1.3.2** **"Business Associate" – is a term specific to UK Link Gemini but for the purposes of this Operating Framework has the same meaning as UK Link User**

**1.3.3** **"Users" is a term specific to UK Link Gemini but for the purposes of this Operating Framework has the same meaning as Authorised Representative**

**1.3.4** **"Party Code/Business Associate Code" is a term specific to UK Link Gemini but for the purposes of this Operating Framework has the same meaning as UK Link User Identity**

**1.3.5** **"User Identity is a term specific to UK Link Gemini but for the purposes of this Operating Framework has the same meaning as UK Link Identity**

**1.3.6** Unless otherwise stated all terms and definitions used in this document shall have the meanings set out in GTD, UK Link Terms and Conditions or Uniform Network Code as applicable.

### 1.4 Scope and Purpose

**1.4.1** The purpose of the UK Link Security Operating Framework is to provide a description of and guidance around;

(a) the operational security procedures and measures as referred to in Clause 7 UK Link Terms and Conditions required to:-

(i) prevent unauthorised access to or use of UK Link; and

(ii) to ensure the protection of UK Link Communications against the risk of resulting alteration, delay, disruption or loss.

(b) as referred to at GT Section D5 Paragraph 5.5.3 the basis on which a UK Link User may nominate representatives as authorised to access and use UK Link on behalf of and using the identification of that UK Link User.

## 2 Roles and Responsibilities

**2.1** This section defines the other principal roles required for the management of UK Link security. The roles are either:-

**2.1.1** Local, that is, they must exist in the organisation of each UK Link User and are concerned with the use of the information and data held within UK Link and/or and the security of each UK Link User's own systems and networks used to access UK Link , or

**2.1.2** Central, that is they are functions concerned with policy, strategic matters and administration of UK Link.

**2.2** The following roles are defined below:

**2.2.1** Local Security Officer (LSO);

**2.2.2** Authorised Representative (AR)

**2.2.3** The CDSP Service Desk;

**2.2.4** Central UK Link Security Administrator;

**2.2.5** Central UK Link Security Manager.

**2.3** Roles should where possible be allocated to separate individuals to reduce conflicts of interest and inadequate segregation of duties in the execution of responsibilities. In some cases it may be expedient to divide a role so that business and information technology responsibilities may be addressed by those with appropriate skills and experience.

**Local Security Officer (LSO)**

**2.4** The Local Security Officer is responsible for

**2.4.1** providing a single point of contact on UK Link security matters

**2.4.2** management of user access to UK Link for the UK Link User for which they are registered as an LSO

**2.4.3** authorisation of all requests to add, amend or remove access to UK Link for individuals within the organisation for which they are registered as LSO

**2.4.4** making all calls regarding account queries such as password resets and/or creation and security matters to the CDSP Service Desk on behalf of the UK Link User for whom it is registered LSO.

**2.4.5** day-to-day liaison with the UK Link Security Administrator and the UK Link Security Manager on UK Link security matters;

**2.4.6** making relevant persons within their UK Link User aware of this Operating Framework;

**2.4.7** monitoring of compliance of the UK Link User for which they act as LSO with this Operating Framework;

**2.4.8** periodic review of the access rights of Authorised Representatives to UK Link;

**2.4.9** reporting security incidents;

**2.4.10** assisting in the investigation of security incidents;

**2.5** Each UK Link User with the exception of CDSP and those set out below is required to have a minimum of two (2) LSO's to ensure cover at all times.

**2.6** The following categories of UK Link User in respect of the following components of UK Link are not required to have LSOs. In these cases the LSO function is performed for those UK Link Users by the CDSP.

**2.6.1** Meter Reading Agents and Utility Infrastructure Providers when using the CMS component of UK Link; and

**2.6.2** Industrial and Commercial Customers and Third Party's when using UK Link Portal.

**Authorised Representatives** ***(GT D5 5.5.3)***

**2.7** Each UK Link User (excluding the CDSP) designates and authorises individuals within their organisations to use UK Link.

**2.8** The process of designating individuals as Authorised Representatives is the responsibility of the UK Link User and is managed and administrated by LSOs

**2.9** The criteria which individuals must meet to be designated as Authorised Representatives is determined by each UK Link User. UK Link Users acknowledge that they are responsible for assessing whether relevant individuals have attained the competence in the use of the UK Link functions to which they are to be granted access and that the CDSP does not make any such assessment.

**2.10** For the UK Link Portal the LSO is responsible for assigning access to UK Link to those Authorised Representatives who are appropriately authorised to use the relevant services within UK Link Portal.

**2.11** The methods, processes and security measures by which Authorised Representatives can access UK Link are prescribed on a service by service basis. Details of each can be found in the relevant sections of this Operating Framework.

**2.12** All Authorised Representatives have a general responsibility to help maintain the security of UK Link and the information or data held in UK Link including Uniform Network Code information. Their responsibilities include taking steps with a view to ensuring that they:

**2.12.1** are aware of this Operating Framework and their organisation's own security policies;

**2.12.2** are aware that they are responsible for all use made of any personal User Identity allocated to them;

(a) safeguard their password by:

(b) choosing a secure and appropriate password, as defined in this Operating Framework;

(c) keeping it secret from everyone else, including their manager;

(d) memorising it carefully rather than writing it down or programming it in any way;

**2.13** are vigilant for misuse of UK Link or information or data held in UK Link and report any suspect activity to their Local Security Officer or their line manager or the CDSP;

**2.14** do not engage in any other activity which is contrary to this Operating Framework.

**CDSP Service Desk**

**2.15** The CDSP Service Desk is the first point of contact on all security matters for LSOs. Its security responsibilities include:

**2.15.1** where the LSO is unable to service a request, the CDSP Service Desk will receive requests from LSOs for changes in system access rights for the Applications for which they are authorised. These requests will be and routed to the UK Link Security Administrator;

**2.15.2** providing a first point of contact for reporting suspected security breaches for UK Link Users excluding the CDSP

**UK Link Security Administrator**

**2.16** The UK Link Security Administrator will action requests by LSOs to provide access for Authorised Representative to UK Link, only where the LSO is unable to service a request themselves.

**2.17** The UK Link Security Administrator may be supported by one or more deputies to ensure cover is provided at all times. The UK Link Security Administrator has overall responsibility

for all actions of his or her deputies. References to the UK Link Security Administrator in this Operating Framework Policy should be read as including Deputy UK Link Security Administrators unless otherwise stated.

**UK Link Security Manager**

**2.18** This role is provided by the CDSP. The UK Link Security Manager provides a central focus and overall responsibility for this Operating Framework and is responsible for:

**2.18.1** providing a single point of contact for UK Link Users on this Operating Framework;

**2.18.2** maintaining this Operating Framework Policy and associated security procedures;

**2.18.3** supporting the management of UK Link on security matters;

**2.18.4** managing information security risks in UK Link;

**2.18.5** development of UK Link security standards and procedures;

**2.18.6** providing overall co-ordination in the investigation of security incidents.

**2.18.7** providing support on security matters for Local Security Officers;

**2.18.8** responding to security incident reports and initiating the incident resolution procedure, including reviewing system audit logs to investigate unauthorised activity.

**General Responsibilities**

## 3 UK Link Access Requirements

**3.1** Access to UK Link will be granted to UK Link Users provided that the UK Link User:-

**3.1.1** (where such UK Link User is a signatory to the Code) has successfully completed the User Admissions Process and been given live status;

**3.1.2** has nominated and registered a Local Security Officer

## 4 Access Control

**4.1** The following principles for communication between the CDSP and UK Link Users are designed to ensure that unauthorised persons do not gain access to UK Link and the information and data held in UK Link:

**4.1.1** all Local Security Officers must be registered with the CDSP;

**4.1.2** the UK Link Security Administrator liaises only with Local Security Officers regarding account queries such as password resets and/or creations;

**4.1.3** the CDSP Service Desk provides the initial point of contact;

**4.1.4** in all communications with the CDSP, Local Security Officers must authenticate themselves.

Each of the above requirements is explained more fully in the sections below.

**4.2** Registration of LSOs

**4.2.1** All LSOs must register with the CDSP in order to make access requests on behalf of a UK Link User.

**4.2.2** The purpose of this registration is to lodge identification details for use by the UK Link Security Administrator which are used to authenticate future communications. This reduces the risk that the UK Link Security Administrator may set access to a UK Link User's information at the request of an unauthorised person.

**4.2.3** The registration details required from the LSO are:

(a) organisation name;

(b) UK Link User Identity (i.e. organisation short code)

(c) full name;

(d) one or more contact telephone numbers

(e) registered email address;

(f) which Application(s) the LSO is responsible for.

**4.2.4** These details will be maintained by the CDSP in the LSO Register. Full details of the registration process are contained in the Local Security Officer (LSO) Registration Form available from the CDSP.

**4.3 LSO as Single Point of Contact**

**4.3.1** The UK Link Security Administrator liaises only with registered LSOs on Security Service Requests.

**4.3.2** Where an LSO requires user identity creation, deletion or amendment for Gemini UK Link, this must be performed using the Security Access Request Form available from the CDSP.

**4.3.3** All other UK Link System applications utilise self-service functionality for LSOs and therefore do not require routing to the CDSP Service Desk. Any other calls to the CDSP Service Desk, which relate to security access, will be refused and users will be required to refer the matter through their LSO.

**4.4 Service Desk as the CDSP Point of Contact**

**4.4.1** The UK Link Security Administrator only deals with security matters when contact is initially made through the CDSP Service Desk.

**4.4.2** Any security incident matter may be reported by any user directly to the CDSP, who will follow the incident management procedure. This ensures that the communication is properly registered and, where necessary, followed up in order to meet the CDSP performance targets.

**4.4.3** The CDSP Service Desk refers communications on security directly to the UK Link Security Administrator, who authenticates the LSO as the originator. The UK Link Security Administrator shall then liaise directly with the LSO when servicing the request.

**4.4.4** The UK Link Security Administrator shall only provide responses pertaining to security access related requests via email to the LSO's registered email address.

### 4.5 Confirmation and Audit of Security Requests

**4.5.1** In all communications with the UK Link Security Administrator, Local Security Officers must authenticate themselves on security matters with the UK Link Security Administrators

**4.5.2** The following rules are applied to communications between the CDSP and LSOs:

(a) If not self-service, details of the Security Service Request from the LSO shall be recorded. The LSO may raise these via telephone or email. The CDSP Service Desk logs all contacts with LSOs by creating a service request ticket.

(b) Email communications must only be sent from the registered email address of the LSO.

(c) The Security Service Request response will ONLY be provided to the registered email address of the LSO, regardless of the method of receipt of the Security Service Request.

## 5 Operational Security Measures *(UK Link Terms and Conditions Clause 7.1)*

**Access to UK Link**

**5.1** Authorised Representatives cannot gain access to UK Link without supplying a valid UK Link User Identity and password. The rules governing the use of UK Link User Identities and passwords is set out in the table at 6.3 below.

**5.2** UK Link contains separate user logins for each of the four UK Link services:

**5.2.1** UK Link Gemini On-line Services (including LSO Administration Facilities);

**5.2.2** Batch File Transfer;

**5.2.3** UK Link Portal (access to UK Link Online Services and Data Enquiry services (DES))

**5.2.4** Contact Management Service (CMS)

**5.3** Summary of UK Link Logins *(**UK Link Terms and Conditions 5.2, 5.4, 5.5 and 7.1.1**)*

| | **UK Link Gemini On-line Services** | **Batch File Transfer** | **UK Link Portal** | **Contact Management Service** |
|---|---|---|---|---|
| **Authentication type** | UK Link Gemini Functions<br><br>User identity and password | UK Link Gateway<br><br>User identity and password | UK Link Online Services and DES access<br><br>User identity and password | CMS Access<br><br>User identity and password |
| **User identity** | | | | |
| Assigned to | UK Link Gemini Functions<br><br>Authorised Representatives (AR) | UK Link User AR or<br><br>External UK Link User AR | UK Link User AR or<br><br>External UK Link User AR | UK Link User AR or<br><br>External UK Link User AR |
| Sharing by ARs permitted? | No | Yes | No | No |
| Concurrent sessions possible? | A single session of each of UK Link Gemini and UK Link Gemini Exit may be run concurrently. | Yes | No | Yes |
| Format | 'External' ARs – (i.e. ARs not within National Grid NTS or the Transporter Agency): XTTTnnn, where X is constant, TTT is the 3 character Short Code denoting the User, nnn is the distinguishing number.<br><br>ARs within National Grid NTS or the CDSP;<br><br>aaa99 or aa999, where aa(a) is the AR's initials and | aaaUSER, where aaa is a UK Link or External UK Link User Identity | The user identities will be system generated based on the users first and last names. If there is already a user within the system with the same first and last name, the system will automatically generate a number against the user identity e.g. JohnSmith1. This number will increment by one for every User in the system with the same first and last | The user identities have a length between 5 and 25 characters.<br><br>It can contain the following special characters (underscore, dash or dot).<br><br>It must not contain spaces or commas.<br><br>Once the user identity is created, is cannot be changed |

| | | | | |
|---|---|---|---|---|
| | 99(9) is a distinguishing number. | | name | |
| Lifetime | Disabled after 90 days if not used. | Unlimited | Unlimited | Unlimited |
| How added | UK Link Gemini Functions<br><br>By UK Link Security Administrator in response to LSO request. | By UK Link Network Support when setting up UK Link Gateway for new UK Link or External UK Link User | LSO creation<br><br>The allocated LSO for an Organisation will create the user, allocate the application services and request service roles | LSO creation<br><br>Xoserve create the LSOs and allocated LSOs can create CMS users |
| How removed | UK Link Gemini Functions<br><br>By UK Link Security Administrator in response to LSO request | By UK Link Network Support on removal of equipment or when LSO notifies as redundant | LSO deletion<br><br>The allocated LSO for an Organisation can permanently delete a user. The LSO can also, disable accounts or remove services without deleting the entire account. Once deleted the user identity and email address cannot be reused. | LSO deletion<br><br>The allocated LSOs for an Organisation can permanently delete a user. Once deleted the user identity and email address cannot be reused. The LSOs can also enable, disable and unlock a user account |
| **Password** | | | | |
| Length | 6-8 characters. | Minimum 6 characters | 8-16 characters | Minimum 8 characters |
| Format | Alphanumeric. LSOs must advise ARs on good practice | No restrictions. | Must contain at least 1 numeric character, 6 alphanumeric characters (A-Z, a-z, 0-9), 1 uppercase character and 1 special character. | Contain a combination of letter and numbers, at least 1 uppercase letter (A-Z), at least 1 number (0-9), at least 1 special character (no spaces allowed).<br><br>When first created as a user, the |

| | | | | |
|---|---|---|---|---|
| | | | | password is system generated |
| Lifetime | 31 days maximum | Unlimited | 45 days | Passwords require resetting every 90 days<br><br>Password change reminder is sent 1 day prior to expiration |
| How changed | Automatic<br><br>AR is prompted on expiry and enters new password<br><br>Manual<br><br>LSO raises a support call on behalf of the AR requesting a reset to be undertaken by the UK Link Security Administrator | By UK Link Network Support in response to request from UK Link or External Uk Link User via the UK Link Security Administrator | Self service<br><br>Upon first access, the User Identity and temporary password are given which prompts a new password request and 3 security questions to be answered.<br><br>Following this, users can change their passwords at any point<br><br>LSOs can also change passwords on a user's behalf | Automatic<br><br>A password change reminder is sent to users 1 day prior to expiration.<br><br>Manual<br><br>user can login to Access Controls and change their password.<br><br>If a user forgets their password, they the LSO can reset it.<br><br>Note: The password cannot be one of the 12 previously used |

## 5.4 Access to UK Link Gemini

Detailed policy for access to UK Link Gemini is provided below under the following headings:

**5.4.1** AR User Identities

**5.4.2** Passwords

**5.4.3** Logins

**5.4.4** Access to Gemini Business Activities

**5.4.5** Access to Gemini Data

### 5.4.1 AR User Identities

UK Link Users are responsible for all actions performed with their AR User Identity(ies). To increase auditability:

(a) User Identities must not be shared by groups of ARs;

(b) User Identities must never be re-allocated to another AR.

The User Identity is used to:

(c) control access by an AR to UK Link Gemini;

(d) control access to business activities and data within Applications;

(e) log the user's actions on the system where required.

Ability to request creation / deletion / amendment of AR User Identities and reset of AR passwords may only be undertaken by the LSO registered with the UK Link Security Administrator for the relevant Application) using the Security Access Request Form available from the CDSP.

**Allocation of AR Access**

(f) An LSO may request a new User Identity and specify its access rights using Security Access Request Form available from the CDSP. The same request is used to modify the access rights of an existing user identity. The process includes actions to:

(i) validate the authenticity of the request;

(ii) ensure that the request is approved by an appropriate LSO;

(iii) set up the requested user profile comprising the roles requested by the LSO, provided it is appropriate to do so;

(iv) issue a User Identity and password to the LSO;

**Validation of AR Access**

(g) Every twelve months, the UK Link Security Administrator issues to LSOs reports listing:

(i) the AR identities currently defined on the system for the User;

(ii) the role(s) available to each AR User Identity.

(h) LSOs are responsible for checking these reports and should notify the UK Link Security Administrator of any errors or redundant AR User Identities via the Security Access Request Form.

(i) LSOs may request such reports more frequently. Such reports may be chargeable.

**Removal of AR Access**

(j) LSOs must contact the UK Link Security Administrator in order to delete User Identities.

(k) LSOs are responsible for requesting the deletion of ARs who no longer require access to UK Link Gemini, for example following resignation, dismissal or transfer to non-UK Link duties. LSOs should use the Security Access Request Form to request deletion of User Identities as soon as they are no longer required.

(l) UK Link Gemini automatically disables user identities for which three consecutive unsuccessful login attempts are made. If a User Identity is not used for 90 days, UK Link Gemini disables the account and the User will be unable to access the account. They will need to request that the account be enabled by the UK Link Security Administrator via their LSO.

### 5.4.2 Passwords [*UK Link Terms and Conditions 5.4, 5.5*]

(a) UK Link Gemini password administration can only be accessed after an Authorised Representative has entered a password known only to him or her. For new user accounts, or following a password reset by the UK Link Security Administrator, the User shall be required to change the password when he or she logs in for the first time.

(b) UK Link Gemini validates passwords to ensure that they meet the requirements set out in the table at 5.3 of this Operating Framework.

(c) LSOs must provide ARs with advice on selecting strong passwords which are both memorable and difficult to guess by others, for example:

(i) by avoiding names of relations, football teams, car registration numbers and other passwords which are closely associated with the individual;

(ii) by avoiding dictionary words;

(iii) by making an AR's new password different from the his or her previous password in at least 4 character positions; and

(iv) by avoiding repeating characters or groups of characters (e.g."AAA", "ABAB").

(d) Passwords are stored so that these cannot be accessed and used in a way that was not intended. Passwords never appear on screens or in any form of printed output.

### 5.4.3 Login

(a) UK Link Gemini displays a screen warning potential users that unauthorised access is not permitted. Following login an AR may change his or her password.

(b) If a User login fails, the user will be informed that the password is invalid. No further information to assist the user.

(c) A timeout operates for each user session. If no activity is detected for a defined period, the session is terminated and the user must log in again. The timeout period is set by default to 120 minutes.

### 5.4.4 Access to UK Link Gemini Business Activities

(a) Access to UK Link Gemini by identified and authenticated users is controlled by allocating ARs to one or more roles, each of which may carry the authority to perform one or more business activities. In UK Link Gemini, roles are known as user roles and business activities are known as functions, corresponding to individual menus and screens. Although an AR may be allocated several roles, he or she must select a single role for use at any one time.

(b) A role may give access to more than one business activity and a business activity may be undertaken by a number of different roles. These are described further in Appendix E – Gemini Security.

(c) Changes to roles and the authorities which they confer are effective immediately after they are made by the UK Link Security Administrator. More information with respect to the roles are provided in Appendix E - Gemini Security.

### 5.4.5 Access to UK Link Gemini Data

(a) UK Link Gemini provides access to the data which an AR can view or update using the business activities available through his or her allocated role(s).

(b) ARs may only enquire on or update certain Uniform Network Code data which relates to a specific UK Link User where they have been assigned to the appropriate Business Associate Code.

(c) Where an AR needs to access data related to more than one Business Associate Code Users must contact the CDSP to enter into arrangements to facilitate such

access. Once appropriate authorisation is received each User Identity for that UK Link User will be assigned access to the relevant Business Associate Code(s).

## 5.5 Access to Batch File Transfer

### 5.5.1 User Identities [*UK Link Terms and Conditions 5.2*]

(a) A single User Identity is allocated to each UK Link User with access to the Batch File Transfer service. This User Identity is used to control access by a User's ARs to the UK Link Gateway.

(b) Each UK Link User is accountable for the use of its User Identity.

(c) LSOs should inform the UK Link Security Administrator of redundant User Identities within 5 working days of their no longer being required.

### 5.5.2 Passwords [*UK Link Terms and Conditions 5.4, 5.5*]

The password is set by the UK Link Security Administrator when the Batch File Transfer service is set up for a User on a UK Link Gateway. UK Link Users are required to implement on their own systems measures (for example a personal user identity and password) which permit access to Batch File Transfer facilities only to authorised personnel.

### 5.5.3 Login

Users of Batch File Transfer must complete a login sequence, regardless of the method (FTP, shared drives etc.) which the user has chosen to access the UK Link Gateway.

### 5.5.4 Access to Business Activities

Business roles are not defined in Batch File Transfer.

### 5.5.5 Access to Data

UK Link Users have the following access to data on the UK Link Gateway:

(a) files sent and received: full read and delete access;

(b) audit trails: read only.

## 5.6 Access to UK Link Portal

The UK Link Portal provides single sign on access to UK Link Online Services and/or Data Enquiry Services depending on a UK Link User's authority to access.

In order for an AR to access the UK Link Portal, they must agree to the terms and conditions of use. If a user does not agree to these Terms, they are not entitled to use the Website and must immediately leave it.

### 5.6.1 AR User Identities

(a) Each account must have a unique user identity assigned.

(b) The CDSP will provide the services of LSO to Industrial and Commercial UK Link Users and Third Partys

(c) LSOs will not be able to manage or see the details from any other organisation. When creating a user the Organisation(s) that can be displayed and selected will only be specific to those that the LSO can act on behalf of.

(d) To create a User Identity, the following information is mandatory:

(i) First Name

(ii) Last Name

(iii) An Email Address

(iv) Organisation

The email address provided does not have to be associated to that individual user; it can be the LSOs email address for example. Please be aware that all notifications regarding a user identity will be sent to the email address registered.

Once a user is created, the services that they are able to see and access through the Xoserve Services Portal is dependent on the services the LSO assigns to them.

#### 5.6.2 Passwords

When a user is created for the UK Link Portal, the user's temporary password is system generated, 2 emails are sent to the user. The 1st will detail their user identity (system generated) and the 2nd will detail their temporary password (also system generated). Upon first access, the user is will be required to enter a new password and three security questions.

The user password must adhere to the defined password policy as set out in the table at 5.3 of this Operating Framework.

#### 5.6.3 Login

When logging into the UK Link Portal, if a user enters their password incorrectly 5 times, their account will automatically lock. In order for a user account to be unlocked, the user must contact one of their LSOs.

In the absence of the LSO, the CDSP can unlock user accounts. However, the first point of call and ultimate responsibility lies with the organisation LSOs.

#### 5.6.4 User Account Management

Once a user account is created, it will not disable/delete automatically despite inactivity. The CDSP will conduct audits on user accounts and engage with Uk Link Users regarding the results.

Whilst this activity will be conducted by the CDSP, it is the LSOs responsibility to manage their user accounts.

### 5.7 Access to Contact Management System

#### 5.7.1 AR User Identities

(a) The User Identity must be unique for each user and cannot be shared or reallocated. It must adhere to the criteria set out in the table at 5.3 of this Operating Framework

(b) The ability to create, delete, amend, enable, disable and unlock AR User Identities and to reset AR passwords may be undertaken by the registered LSO.

(c) The registered LSO for a UK Link User is responsible for creating a user and assigning the correct organisation and provisioning the required services. To create a user the following information is mandatory:

(i) First Name

(ii) Last Name

(iii) User Identities

(iv) Email Address

(v) Organisation

(d) Once created, the user account will not disable after any period of inactivity. It is the responsibility of the LSOs to manage any user accounts no longer in use.

### 5.7.2 Passwords

(a) When a CMS user is created, the user's password is system generated.

(b) Once successfully created, 2 emails are sent to the user of the newly created account. The 1st will detail their user identity and the 2nd will detail their system generated password.

(c) An AR may change his or her password at any time. The system will send an automatic 'Password Change' reminder, 1 day prior to the expiration.

(d) CMS validates passwords to ensure that they comply with the requirements set out in the table at 5.3 of this Operating Framework

### 5.7.3 Login

(a) Following login an AR may change his or her password by accessing 'My Account' details.

(b) When logging into the system, if a user enters their password incorrectly 3 times, their account will automatically lock. It is the responsibility of the LSO to unlock the account.

# 6 AUDIT TRAILS

**6.1** This section describes the audit trails and information retained to provide a record of Uniform Network Code communications.

**6.2** The CDSP must retain a complete and chronological record of UK Link Communications for the relevant periods as defined below.

**Audit Trails Provided by UK Link System**

**6.3** Audit trails are recorded by several of the elements of UK Link at the point at which the auditable activities occur. For example:

(a) Successful UK Link Gemini on-line transactions are recorded;
(b) Information about batch files transferred to or from UK Link Users
(c) the Active Notification System (ANS) records messages sent;
(d) Changes to a UK Link Users and AR User Identities and passwords are recorded by the security components.

Each of these audit trails is described below.

**Retention of Audit Trails (*GTD5.8.1)***

**6.4** The CDSP retains data in line with the CDSP retention policy and will retain audit trails so that these are attributable to AR where relevant.

**Provision of Audit Trails to UK Link Users**

**6.5** Information may be retrieved by one of the following methods, depending on the facilities available in UK Link component which maintains it:

**6.5.1** ***information currently retained on-line:***

(a) by on-line enquiries;
(b) by on-line request of batch reports;
(c) by written request to UK Link Security Manager to obtain reports;

**6.5.2** ***information currently retained in archive***:

(a) by written request to UK Link Security Manager to obtain reports.

**6.6** LSOs should submit written requests to the UK Link Security Manager stating what is required and for what reason. The CDSP reserves the right to make a charge for providing copies of audit trails.

**6.6.1** UK Link Users may only request relevant sections of an audit trail comprising records relating to:
**6.6.2** access to and use of UK Link by the UK Link User's own ARs;
**6.6.3** access to and use of UK Link from any person via the UK Link User's Gateway;
**6.6.4** access to and use of the UK Link User's data by any person;
**6.6.5** transmission of files to and from the UK Link User.

**6.7 UK Link Gemini**

### 6.7.1 Description

A complete audit trail of the on-line communications between the CDSP and the UK Link User is provided through database transaction audit trails which record:

(a) details of the enquiry and update transactions executed by ARs (further detail is provided in section 4.3.2);
(b) changes to UK Link Gemini roles, business activities, and authorities by the UK Link Security Administrator;
(c) the retention of Uniform Network Code data in the UK Link Gemini database, which allows information previously communicated to be obtained retrospectively by either party;
(d) changes to user identities and passwords by the UK Link Security Administrator.

### 6.7.2 Transactional Audit Trail [GTD5.8.1]

The information is captured within the transaction processing system. The audit trail includes:

(a) the action which was taken (create, update, delete, send, receive);
(b) the data which was affected (which fields, records or files);
(c) the identity of the AR performing the action;
(d) the date and time at which the action was taken.

### 6.7.3 Database Information [GTD5.6.2]

UK Link Gemini retains a history of all communications containing a UK Link User's final committed values on each gas flow day.

This history is retained on-line in the database for a limited period during which it is available for enquiries. UK Link Users may request some reports via on-line facilities. In other cases it is necessary to submit a written request to the CDSP.

## 6.8 Batch File Transfer

### 6.8.1 Description

A complete audit trail of information about the batch communications to and from the UK Link User is provided by:

(a) the UK Link Network audit log (described in further detail in 6.8.2);
(b) copies of the transmitted files retained for a limited period on the Gateways (described in further detail in 6.8.3);
(c) copies of the transmitted files retained by UK Link (described in further detail in 6.8.4).

### 6.8.2 UK Link Network Audit Log [GTD5.8.1]

The UK Link Network audit log contains details of actions on all files sent from and received by the UK Link User. The following information is recorded:

(a) name of the message file;
(b) action taken: sent, received, re-tried etc.;
(c) whether successful or unsuccessful;
(d) date and time of action.

The audit log recorded on the UK Link User's Gateway can be read by the UK Link User. The CDSP reads the logs from all UK Link Users' Gateways across the network and consolidates these into a single log accessible by the CDSP.

### 6.8.3 Files Retained on Gateway

A copy of each file sent from the CDSP is retained:

(a) on the CDSP Gateway for a period of ten calendar days;
(b) on the user's Gateway for a period of ten days or until the files are deleted by the user, whichever is the sooner.

A copy of the files sent by the UK Link User is retained on the UK Link User's Gateway as defined in the UK Link File Transfer Guide or until the files are deleted by the User, whichever is the sooner.

### 6.8.4 Files Retained by UK Link (*GTD 5.8.1*)

A copy of the files sent and received by the CDSP is retained on the UK Link System in accordance with the CDSP data retention policy.

## 7 Security of Connected Systems

**7.1** This section describes technical security measures which each UK Link User shall implement in respect of any systems connected via the UK Link Network to UK Link. The purpose of these measures is to prevent a poorly controlled system placing other systems in the UN Link Network at risk of unauthorised access (either intentionally or accidentally).

**7.2** The security controls in UK Link support best practice requirements as set out in ISO27001.

**7.3** The CDSP shall undertake formal risk assessments of the security controls in UK Link at least every two years to assess the adequacy of such security controls and identify areas where improvements may be necessary.

**7.4** It is strongly recommended that UK Link Users to ensure that their local security policies are compliant with ISO27001.

**7.5** UK Link Users should take all reasonable and prudent steps to prevent, by the use of firewalls or other means, the possibility of any communications between the UK Link Network and any other external network, including the Internet, being accessed inappropriately.

**7.6** UK Link Users are responsible for all access to the UK Link System originating from or routed through its physical location whether authorised or not.

**7.7** UK Link Users, should take all reasonable and prudent steps to protect itself against unauthorised access to its systems and networks via the UK Link Network.

**Requirements for Systems Connected to UK Link**

**7.8** UK Link Users may implement firewalls between their UK Link Gemini Gateway/Router and their own network. Although UK Link may need to be configured to recognise the existence of the firewall, administration of the firewall is entirely the responsibility of the UK Link User.

**7.9** Uniform Network Code data is not encrypted whilst passing over the UK Link Network. UK Link Users are therefore advised to implement appropriate measures to safeguard data passing over their local area networks.

**Requirement for Automatic Login by Software**

**7.10** UK Link Users and External UK Link Users may implement an automatic login to UK Link Gateway, in which the User Identity and password are hardcoded into the software on the connected system. All of the requirements in this Operating Framework must be met by User Identities and passwords used in this way and the UK Link User to which they have been allocated remains responsible for their use.

**Security of physical Equipment**

**7.11** Much of the information held on the Gateway will be commercially sensitive and therefore for both security and insurance purposes UK Link Users should ensure that the equipment is housed in a secure area. Any keys which give access to the equipment must be kept in a secure place and authorised staff of the CDSP or its subcontractors must have on-site access to the keys for maintenance and support purposes.

## *8* Virus Protection *(UK Link Terms and Conditions 7.2)*

**8.1** UK Link Users are required to have procedures in place to prevent harmful code or programming instructions from being transmitted to one another, or where received, to ensure that such code has no impact. Guidance regarding the minimum processes and procedures that should be in place for each UK Link User are set out below: -

**8.1.1** incoming media and communications should be checked for viruses before any data and/or software is read into the destination system or the contents of the media are displayed;

**8.1.2** installing as soon as is reasonably practicable any associated patches provided by software / hardware vendors to maintain the integrity of the system components.

**8.1.3** appropriate network level protection to identify and prevent unauthorised access

**8.1.4** Implementation of measures to check both incoming and outgoing batch messages for viruses. Outgoing messages should be checked at the last practicable point prior to placing the message on the UK Link Gateway for transmission to the other party. Incoming messages should be checked at the first practicable point after retrieving the message from the UK Link Gateway and before the data and/or software is loaded into the receiving system.

**8.2** The CDSP implements additional measures with the aim of ensuring that UK Link remains free of malicious software. The CDSP will provide appropriate security controls prior to installation of UK Link Gateways and will conduct periodic sweeps of the servers.

### 8.3 Notification of Virus Contamination [*UK Link Terms and Conditions 7.2 (b)]*

**8.3.1** If a UK Link User, suspects virus contamination, then no further attempts must be made to read batch data from or write batch data to the UK Link Gateway. The LSO

must report the infection to the UK Link Security Administrator according to the Security Incident Resolution procedure set out in this Operating Framework.

**9 Notification of Unauthorised Access (*UK Link Terms and Conditions 7.1.3 –7.1.5*)**

**9.1** Notification of unauthorised access to UK Link shall follow the process set out at section 10 of this Operating Framework.

**10 Security Incidents** (***UK Link Terms and Conditions 7.1.2 – 7.1.5 & 7.2 (b)***)

**10.1** A security incident is a suspected security failure. The facts are established by subsequent investigation. LSOs should ensure that all ARs are aware of what constitutes a security incident.

**10.2** The details of the actions to report and resolve security incidents are described in the procedure Security Incident Resolution.

**10.3** The incidents which must be reported include:

**10.3.1** unauthorised access to the UK Link System or any information;

**10.3.2** access to information which should not be permitted by virtue of an Authorised Representative's role;

**10.3.3** misuse of User Identities (e.g. sharing);

**10.3.4** receipt of information intended for another UK Link User;

**10.3.5** illegitimate use of UK Link information (e.g. disclosure to third parties);

**10.3.6** computer virus contamination;

**10.3.7** unauthorised modification of UK Link information;

**10.3.8** malfunction of security controls in UK Link;

**10.3.9** tampering with UK Link equipment

**10.3.10** unauthorised changes to the UK Link software or to the configuration of the UK Link hardware or networks

**10.3.11** any other incident which could result in alteration, delay, disruption or loss of UK Link information.

**UK Link Users (*UK Link Terms and Conditions 7.1.2, 7.2 (b)*)**

**10.4** If a UK Link User becomes aware that the security of UK Link has, or has been potentially compromised, the LSO must immediately notify the CDSP by telephone to the CDSP Service Desk.

**The CDSP (UK Link Terms and Conditions 7.1.3, 7.2 (b))**

**10.4.1** If the CDSP detects that the security of UK Link has been compromised, it must notify all UK Link Users affected immediately.

### 10.5 Security Incident Resolution (*UK Link Terms and Conditions 7.1.4, 9.1.1*)

**10.5.1** UK Link Users, and the CDSP must take reasonable steps to assist each other in the investigation and resolution of security incidents. Each UK Link Users and the CDSP shall bear their own costs in any such investigation.

**10.5.2** In addition to the provisions of the UK Link Terms and Conditions, section 9.1.1, with respect to disconnection of a UK Link User, the CDSP is entitled to withdraw access from an individual AR with immediate effect if it has reasonable grounds to believe that a breach of security has occurred.

**10.5.3** The AR cannot log in to UK Link Gemini after access is withdrawn and the AR's access cannot be restored by the LSO. In these circumstances the CDSP discusses the position with the LSO and agrees if and when access should be restored.

**10.5.4** The UK Link Security Manager further co-ordinates the response to any security incident by:

(a) notifying all affected parties by relevant means. This includes all UK Link Users:
  (i) which own information which has been accessed;
  (ii) to which the accessed information relates, if different.

(b) immediately taking action:
  (iii) to prevent a repetition of the security failure;
  (iv) to restrict the impact of the security failure;

(c) launching an investigation into the cause of the security failure, with the assistance of LSOs where required;

(d) discussing with UK Link Users possible steps to reduce the risk of further unauthorised access;

(e) implementing agreed solutions;

(f) notifying all UK Link Users of the action taken.

## 11 Data Protection

**11.1** For the purposes of this section 11 Data Protection Legislation means the Data Protection Act 1998 and any successor to such legislation including but not limited to General Data Protection Regulation (EU) 2016/679)).

**11.2** Each UK Link User acknowledges that UK Link contains Personal Data as defined by the Data Protection Legislation.

**11.3** Each UK Link User is responsible for ensuring that it complies with Data Protection Legislation in respect of any Personal Data which it processes on its own computer systems, including those connected to UK Link via its UK Link Gateway/Router.

**11.4** Each UK Link User shall only use the Personal Data held in UK Link in accordance with UK Link Terms and Conditions and in such a way as is compatible and consistent with its duties and obligations under Data Protection Legislation.