Procedure Name:	***Vendor Access Management Procedure***
Procedure Ref:	PRO/SC/VA/IT/0009
Who it applies to:	Staff, Volunteers, Directors, Board Members, Trustees, Members and/or other Associated Persons.
Date of issue:	June 2019
Last revised Date:	April 2023
Review date:	December 2024
Version:	1.2
Procedure Type:	Internal
Procedure Owner:	Director of Business Transformation
Approved by:	Corporate Policy Review Panel (CPRP)
Company Policy relates to:	Group

Vendor Access Management Procedure

Vendor Access Management Procedure

Contents

1 Introduction

This Procedure informs CILEX Management, Business Owners, IT and Support Staff of the CILEX requirements for Vendor Access to Channel Service Unit/Data Service Unit (CSU) Information Systems. It defines the Vendor's responsibilities for the protection of CSU Information and Information Systems.

This Procedure applies to all individuals and/or parties that are responsible for the installation of new CILEX Information System Assets, the operations and maintenance of existing CILEX Information Systems and who do or may allow Vendor Access for support, maintenance, monitoring and/or troubleshooting purposes.

2 Vendor Access

Vendor access to CILEX SU Information Resources is granted solely for the work contracted and for no other purposes.

Vendors must comply with all applicable CILEX Policies, Practice Standards and Agreements, including, but not limited to:

- Privacy Policy
- Data Protection Policies
- Information Technology Policy and Procedures

3 Vendor Agreements and Contracts

Vendor Agreements and Contracts must specify:

- The adherence of the Vendor to all CILEX Policies, while working for it;
- Details of the CILEX information the Vendor should have access to. If, at the time of the contract negotiation this is unknown or ambiguous, then a mention of this should be made in the Agreement;
- How CILEX information is to be protected by the Vendor. A copy of the Vendor's Security and Privacy Policy should be made available to CILEX, where appropriate and if the use of Personal Data is involved, then a Data Processing or Data Sharing Agreement should be signed, in addition to the contract, which will be produced by the Corporate Compliance Team;
- Acceptable methods for the return, destruction or disposal of CILEX information in the Vendor's possession at the end of the contract;
- Agreement that the Vendor must only use CILEX's information and Information Systems for the purpose of the business agreement;
- Any other CILEX information acquired by the Vendor, in the course of the contract cannot be used for the Vendor's own purposes or divulged to others.

Where applicable, IT Support will provide a technical point of contact for the Vendor. The point of contact will work with the Vendor to ensure that the Vendor complies with CILEX Policies.

Where applicable, the Business Owner will provide the Vendor with a point of contact from within the relevant Department/Company. The internal point of contact is responsible for liaising with IT for all relevant Change Management Processes.

Vendor Personnel must report all security incidents directly to the appropriate CILEX point of contact. The CILEX point of contact shall immediately notify the Group Privacy Officer about these incidents.

If Vendor Management is involved in CILEX Security Incident Management, the responsibilities and details of involvement must be specified in the contract.

The Vendor must follow all applicable CILEX Change Control Processes and Procedure.

Before the commencement of the agreement, the appropriate implementation of CILEX Change Management Process will be determined by CILEX, in consultation with the Vendor and the Group Business Owner. This will include such things as the definition of standard changes, level and type of communications around changes and the responsibilities around Technical Vulnerability Management and IT Security Incident Reporting.

At the commencement of the agreement, Standard Changes, as defined in the context of the CILEX Change Management System must be clearly identified and agreed upon by the Business Owner, the Vendor and IT.

When appropriate, Vendors shall provide assistance to their CILEX point of contact and the Group Privacy Officer with the development of the Data Protection Impact Assessment (DPIA).

If appropriate, regular work hours and duties will be defined in the contract. Work outside of defined timeframes must be approved by the appropriate CILEX Business Owners.

4 Change Management System

All work and changes that are identified, as impacting on other CILEX systems must be entered into the CILEX Group IT Change Management System by the CILEX point of contact or where applicable, the Business Owner point of contact. Activities include, but are not limited to, such events as software/operating system updates/patches, password changes, project milestones, changes to deliverables and the commencement and completion times, wherever possible.

The Vendor's work activities on CILEX systems may be monitored and logged for comparison to the Change Management System Records.

Before the commencement of the agreement, methods for the monitoring and review of service performance, logging activities, submission of Vendor reports and the roles and responsibilities regarding problem management will be determined by CILEX, in consultation with the Vendor and the Group Business Owner.

5 Information Provided by the Vendor

Each Vendor must provide CILEX with a list of all employee names working on the contract. The list must be updated and provided to CILEX within 24 hours of staff changes, wherever possible.

Each Vendor Employee with access to CILEX sensitive information must be cleared to handle that information.

6 Vendor Access

Vendor access must be uniquely identifiable and password management must comply with the CILEX Password Policy and the CILEX Remote Access Policy.

All Vendor maintenance equipment on the CILEX network that connects to the internet via any means and all vendor accounts will remain disabled, except when in use for authorised maintenance.

7 End of Contract

Departure of a Vendor or Vendor Employee from the contract for any reason, the Vendor will ensure that all sensitive information is collected and returned to CILEX or destroyed within 24 hours.

Upon termination of the contract or at the request of CILEX, the Vendor will return or destroy all CILEX information and provide written certification of that return or destruction within 24 hours.

Upon termination of contract or at the request of CILEX, the Vendor must surrender all CSU access cards, badges and equipment immediately. Equipment and/or supplies to be retained by the Vendor must be documented by authorised CILEX Senior Management.

8 Requirements to Vendors

Vendors are required to comply with all regulatory and CILEX auditing requirements, including the auditing of the Vendor's work. The Vendor's must adhere to UK Legislation and Regulations, including the UK Data Protection Legislation.

All software used by the Vendor in providing a service to CILEX must be properly inventoried and licensed.

Each Vendor granted access to any CILEX Information System must sign its adherence to the relevant CILEX Policies that pertain to the access required. This would be recorded and stored by the IT Department via Email/SharePoint.

9 Breach of IT Security Incident Management Procedure

Individuals in breach of this Procedure are subject to the CILEX Disciplinary Procedure. CILEX will take legal action to ensure that its information systems are not used by unauthorised persons.

When personal information has been unintentionally disclosed, this should be immediately reported to the Group Privacy Officer with the completion of the PDSI Form, in accordance with the Potential Data Security Incident Reporting Policy.