Supplier Information Security Policy

Cornerstone Document Reference – CS-IS-POL-21

Cornerstone, Hive 2, 1530 Arlington Business Park, Theale, Berkshire, RG7 4SA

Registered Address: Cornerstone Telecommunications Infrastructure Limited, Hive 2, 1530 Arlington Business Park, Theale, Berkshire, RG7 4SA
Registered in England & Wales No. 08087551. VAT No. GB142 8555 06

Purpose and scope

The purpose of this policy is to ensure that all contracts and dealings between Cornerstone and third-party suppliers have acceptable levels of information security in place to protect personal data as defined by the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018. These requirements are in line with Cornerstone's Information Security Management System (ISMS), current data protection legislation and information security best practice. This policy sets out Cornerstone's expectations in respect of information security when engaging with third party suppliers.

Usually, the relationships between Cornerstone and its' third-party suppliers are ultimately governed by the contract or information sharing agreement, which is entered into between Cornerstone and the third-party supplier.

The scope of this policy applies to all agreements that involve IT solutions or provision of services which require access to, or the processing of, personal data for the delivery and/or support of Cornerstone services and business functions. The term 'Data' within this policy refers to either:

a) the storing, handling, processing, or retention of data including personal data related to Cornerstone's information. Examples include the procurement of major IT solutions for Payroll, Site / Estate Management, HR etc, or

b) the storing, handling, processing, or retention of data - including personal data related to/associated with the services commissioned by Cornerstone.

Information Security Risks and Requirements for Third Party Suppliers

The security of information is the key focus in Cornerstone's ISO27001 risk assessment, procurement and management strategy. Cornerstone uses a risk based and proportionate approach to how information assets should be protected. Cornerstone may request from third party suppliers' access to perform site assessments, document exchanges, copies of procedures and policies, security assurance reports and third-party audits to determine the suitability of Third Party Suppliers security controls.

A protocol has been developed for use in the procurement of all contracts, including those which will hold personal data. The use of this protocol is driven by the nature of the service and information processing, its criticality to Cornerstone's value chain and the sensitivity, volume and risk associated with the information held. This will include ensuring the new Supplier completes a Supplier Security Assessment Questionnaire (SSAQ), which meets with the approval of the Information Security Officer (ISO) or their delegate the Information Security Manager (ISM).

Furthermore, where Cornerstone is performing a supplier renewal, records should be checked to determine when the supplier last completed an SSAQ. If three years have elapsed since the last SSAQ was completed then the Procurement team will request that the supplier review their SSAQ, update it accordingly and reissue the SSAQ.

The Supplier Security Assessment Questionnaire CS-IS-FM-01 can be found in the DMS. In addition all Third Party Suppliers () supplying IT services as described under Appendix 1 Software Development Security Requirements, or where the third party is signing Cornerstone's standard framework agreement, should have ISO27001 accreditation or a commitment to obtain ISO27001 certification within 12 months of signing an agreement with Cornerstone and thereafter for the duration of that agreement. Any deviation of this should be reviewed and approved by the ISO or their delegate, refer to section Deviations from Policy.

The completed SSAQ and any other supporting material such as certificates, policies and security reports will be stored in the Teams Information Security under sub folder InfoSec Supply Chain Management.

Information Security requirements will also be included in any Project Business Requirement and/or Solutioning documents and will require approval by Gating. Security requirements are typically recorded in the Business Requirements Document, refer to section Related Documents.

Third Party Suppliers providing, integrating and/or developing software, applications, and systems to Cornerstone must ensure that such supplies abide by the security requirements detailed in Appendix 1 Software Development Security Requirements.

Cloud Service Providers

To mitigate the risks associated with cloud service providers, Cornerstone has determined that cloud services must not only be selected in accordance with the broader supplier selection process, but also the evaluation must consider:

- The availability of the service.
- The location where data will be stored.
- The process for data removal from the service.
- The personnel within the provider who will have access to the data.
- The provider's notification procedures for incidents.
- The provider's compliance with broader ISMS policies, including those related to passwords, encryption, and network security.

Cloud service providers must possess ISO 27001 or an equivalent internationally recognized certification. If a cloud provider lacks such certification, a risk assessment must be conducted by the ISO, ISM, or a member of the IT management team.

Contracts

Contracts shall clearly define each party's information security responsibilities toward the other by detailing the parties to the contract, effective date, functions or services being provided (e.g. defined service levels), liabilities, limitations on use of subcontractors and other commercial/legal matters normal to any contract. Depending on the results of the risk and impact assessment for each supplier, various additional information security controls may need to be put in place in addition to the standard ones, depending on the nature of the service provision.

Management of Supplier Relationships

During the term of a contract with a Third Party Supplier, Cornerstone will manage the arrangement with the third-party supplier to ensure Information Security standards are maintained.

Supplier Access to Cornerstone Information

Cornerstone will allow third party suppliers to access its information and data, in accordance with the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018, Cornerstone's ISMS and where:

- Accessing the information is an agreed part of the solution/service provided.
- The processing and viewing of information is necessary for maintenance and troubleshooting of the solution being provided.
- Information may need to be reconstructed, repaired, or restructured.
- Information has been provided for inclusion in the solution/service by Cornerstone.
- Information may need to be transferred to other systems or during IT solution upgrades.
- Information may need to be collected with agreement from, and on behalf of, Cornerstone.

Viewing (i.e. access not agreed by Cornerstone) of Cornerstone information is not permitted at any time by third party suppliers. Cornerstone information must not be accessed under any circumstances unless formal information sharing agreements or written contractual permissions have been established between the parties which permit this to happen.

The extent of third-party supplier requirements to access Cornerstone information will need to be identified prior to any contractual obligations being established and entered into. The level and type of access to Cornerstone information by Third Party Suppliers must also be formally agreed by the parties. The security requirements for each type of information will be defined by

the Information Security Officer or their delegate, and the security of the information must be handled in accordance with Cornerstone's Information Classification and Handling Policy. Business owners responsible for managing the ongoing relationship with a Third Party Supplier will be encouraged to include security agenda items as part of their periodic service review meetings, this will typically include security incidents and changes to user access.

Cornerstone is very clear that where there is a requirement for the processing of personal data of employees or service users' information by third parties, information will be treated in accordance with Cornerstone's requirements to ensure the confidentiality, integrity and availability of all information.

Supplier Audit & Site Visits

As part of Cornerstone's commitments under the Data Protection Act 2018 and its ISO27001 accreditation Cornerstone may seek to undertake an independent Audit of any Third Party contracted to provides services to Cornerstone. The Supplier Audit review may necessitate a visit to the third-party supplier's data centre and/or main office where access to, or processing of, personal data is being undertaken on behalf of Cornerstone. The findings of any Supplier audit will be summarised using either the High, Medium or Low Level Supplier Audit Form and any audits will be carried out in accordance with the Information Security Audit Process CS-IS-PR-05, refer to section Related Documents. The objective of the site visit(s) will be to assess the adequacy of the physical, logical, and operational controls in place and assess whether the supplier's approved IT security procedures are embedded within daily operations.

Security Incident Management

Third party suppliers will be expected to have appropriate security incident management procedures in place, which correspond to the level of service being provided, and sensitivity of the data. The extent of these responsibilities will be specified in the contract or data sharing agreement. Third party suppliers will be required to notify Cornerstone of any significant security incidents as soon as practical.

Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Cornerstone information assets, or an event which is in breach of Cornerstone's security procedures and policies. All Third Party Suppliers contracted to provide, support or access solutions, which enable Cornerstone to carry out its business functions and deliver its services, have a responsibility to adhere to this policy and all supporting requirements as described and referenced within formal documentation and agreed contractual agreements.

All employees have a responsibility to report security incidents and breaches of this policy as quickly as possible through Cornerstone's Incident Reporting Procedure.

In the case of third-party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to IT solutions or suspension of contractual arrangements. If damage or compromise of Cornerstone's IT solutions or loss of information results from the non-compliance, Cornerstone will consider legal action against the third party. Cornerstone will take appropriate measures to remedy any breach of this policy and its associated procedures and guidelines through the relevant contractual arrangements in place or otherwise via statutory processes.

This document forms a fundamental part of Cornerstone's ISMS and as such, must be fully complied with.

Deviations from Policy

Unless specifically approved, any deviation from this policy is strictly prohibited and should be raised as an exception. Any deviation to or non-compliance with this policy shall be reported to the Information Security Officer or delegate for review.

Related Documents

Supplier Security Assessment Questionnaire CS-IS-FM-01
Low Level Information Security Supplier Audit Form CS-IS-FM-07
Medium Level Information Security Supplier Audit Form CS-IS-FM-06
High Level Information Security Supplier Audit Form CS-IS-FM-05
Information Security Audit Process CS-IS-PR-05
Cornerstone Information Security Policy CS-IS-POL-01
Business Requirements Document CS-IT-DC-05
Procurement Policy CS-SCM-POL-107

Glossary of Terms

The following table is a list of abbreviations and terms used in or related to this policy and the meaning of them.

Abbreviation / Term	**Meaning / Definition**
Third Party Supplier	Provider of supplies and services to Cornerstone.

Supplier	Third Party Supplier
TPS	Third Party Supplier

Appendix 1 Software Development Security Requirements

Third Party Suppliers (TPS) providing, integrating and/or developing software, applications, and systems to Cornerstone must ensure that such supplies abide by the security requirements detailed in Appendix 1 Software Development Security Requirements.

a. TPS to ensure documents sent to Cornerstone are suitable, adequate, and effective.

b. TPS to ensure the protection of information from unauthorised access or disclosure (Confidentiality)

c. TPS to ensure the protection of information from unauthorised modification or destruction (Integrity)

d. TPS to ensure the protection of information from unauthorised disruption (Availability)

e. TPS to ensure strong user authentication mechanisms requiring two/multi factor authentication (2FA/MFA) for user login to all supplied systems.

    i. 2FA/MFA must be configurable to remember multi-factor authentication on trusted devices between 0 to 365 days.

    ii. 2FA/MFA must allow users to remember multi-factor authentication on devices they trust.

f. Data Encryption

    i. TPS must ensure all data transfer and handling to be secure, encrypted and GDPR compliant by way of using https with tls1.2 and/or 1.3.

    ii. TPS will work with Cornerstone to define the sensitive data that may need to be registered in the Supplier systems (if not anonymised). TPS will then define with the protection (visibility by administration levels) and retention.

    iii. TPS must ensure all stored data/data at rest (e.g. in disks, volumes, and databases), which is classified as sensitive or personal data, will be adequately encrypted.

g. Portal security/ web and user interface infrastructure access and data encryption

    i. TPS must ensure all the communication will be encrypted as per the above data encryption standards

    ii. TPS must ensure all data is synchronised securely across all Supplier products via secure channels.

iii. TPS applications will restrict access to only those Cornerstone, shareholder or third-party employees granted access.

iv. TPS must ensure Cornerstone employee's authentication will be implemented using ADFS Single Sign-On (SSO) and, where requested, multi factor authentication (MFA).

v. TPS must ensure that authentication for all external users to Cornerstone, will be implemented using MFA.

h. Time out security measures

i. TPS must ensure that session timeouts are configured to an appropriate duration appropriate to the sensitivity of the data that might be exposed. This can vary from 15 to 30 minutes, with the lower end of the scale reflecting higher sensitivity of data.

i. Design/development of the Supplier products

i. TPS must ensure that data confidentiality and integrity in respect of the TPS Systems used to deliver the Services is of paramount importance and the security requirements of the supplied systems must be designed, deployed, and managed as such.

ii. TPS must adopt and implement security design and development principles which incorporate good industry practices for secure design and development such as OWASP methodology

iii. TPS must comply with the standards set out in Cornerstones Secure Software Development Lifecycle in addition to any of the requirements listed herein.

j. Security Testing

i. TPS is required to perform non-functional security testing, also known as penetration testing, prior to the release or deployment of software, code and applications into production. This is to uncover potential vulnerabilities resulting from coding errors, bad system configuration, or other operational deployment weaknesses.

ii. TPS should perform security testing by way of identifying security vulnerabilities (security defects), fixing the defects, revalidating to confirm defects are fixed and providing a final report listing security defects

identified and mitigated, including but not limited to, information relating to the defect, location and the perceived threat/risk.

iii. TPS must ensure that all remedial action required to fix security defects shall be:

1. Accompanied by a remedial action plan including specific objectives and timetable for completion.
2. Verified and agreed with Cornerstone in advance.
3. Wholly and completely implemented at the Suppliers expense.

iv. TPS must ensure security testing methodology follows recognised industry standards such OWASP Top 10 or an equivalent standard.

v. TPS must perform ongoing and on at least an annual basis security testing on supplied systems retaining, transmitting, protecting, or processing Cornerstone Information and provide the results of all such testing to Cornerstone (in writing).

k. User roles and responsibilities

i. TPS must ensure user authorisation to resources, objects and interfaces are managed through Role Based Access Controls (RBAC).

ii. TPS must ensure roles are configured according to the principles of least privileges.

iii. TPS must ensure segregation of duties and users

l. System Security Patching and Configuration

i. TPS must ensure a suitable security patch management process to ensure the ongoing integrity of Systems supplied and which shall be regularly updated in accordance with Good Industry Practice.

ii. TPS must ensure the security configuration of supplied systems is in accordance with Good Industry Practice (e.g. Centre for Internet Security benchmarks) and provide evidence of such security configuration to Cornerstone (in writing).

iii. TPS must ensure the physical or logical segregation of systems supplied to Cornerstone from other supplier customers.

m. Audit Logs and Monitoring

i. TPS must ensure system auditing is configured to record:

i. Start and stop of system processes

ii. Use of privileged capabilities or change in privilege

iii. Login success and failure, to include.

1. Unique user identification
2. Date and time stamp
3. IP address / hostname

ii. TPS must ensure system audit logs are kept for a minimum of 12 months, with the last 3 months immediately available and 9 months prior archived.

iii. TPS must ensure time and date stamps must be derived from a central Network Time Server e.g. NTP.

iv. TPS must ensure audit logs are saved in a structured and commonly acceptable standard e.g. syslog files.

v. TPS must ensure the integrity of audits logs by enforcing tamper proofing measures.

vi. TPS must monitor events for security threats, attacks or potential breaches and notify Cornerstone within 24 hours of identifying such security breach