|  |
| --- |
| **External IA Evaluation Diligence**  Information Gathering for Cloud & External Systems Hosting |
| Date: 09 July 2019 |
| Version: 6.0 |
|  |
|  |

Contents

[Summary – The Purpose of This Document 3](#_Toc5110027)

[Guidance for Completion 4](#_Toc5110028)

[Commitment of Completion 4](#_Toc5110029)

[01 - Data in Transit Protection 5](#_Toc5110030)

[02 - Asset Protection and Resilience 5](#_Toc5110031)

[03 - Separation of Users 8](#_Toc5110032)

[04 - Governance Framework 8](#_Toc5110033)

[05 - Operational Security 9](#_Toc5110034)

[06 - Personnel Security 11](#_Toc5110035)

[07 - Secure Development 12](#_Toc5110036)

[08 - Supply Chain Security 13](#_Toc5110037)

[09 - Secure Consumer Management 14](#_Toc5110038)

[10 - Identity and Authentication 14](#_Toc5110039)

[11 - External Interface Protection 15](#_Toc5110040)

[12 - Secure Service Administration 15](#_Toc5110041)

[13 - Audit Information Provision to Consumers 16](#_Toc5110042)

[14 - Secure use of the service by the consumer 17](#_Toc5110043)

**Version History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Details** |
| 0.1 | 17/01/2012 | Angus Macrae – Prior cloud doc draft for group review |
| 1.0 | 18/01/2012 | Prior cloud doc Post review versioned |
| 2.0 | 09/05/2014 | New title ‘External Systems Hosting – IA’ and major revision of all sections |
| 3.0 | 31/07/2015 | First version as new document aligned with CESG principles |
| 4.0 | 08/10/2018 | Aligned with NCSC 14 cloud principles |
| 5.0 | 05/04/2018 | Minor updates |
| 6.0 | 09/07/2019 | Updated the summary |

Summary – The Purpose of This Document

This document is intended for completion by external solutions providers as an initial information gathering tool only. Its purpose is to assist the Council when ascertaining the suitability of an externally hosted IT or Software Application solution. It will further be used to inform assessments of residual risk where special categories of data is being processed.

The document uses structural alignment and direct reference from the NCSC (National Cyber Security Centre) Cloud Security Principles. These principles are designed to give guidance to cloud service providers and is considered good practice to adhere with these principles and the relevant accreditations.

Wherever an external solution is to be considered for processing personal data, the Council as the Data Controller, must ensure that any third party to whom they delegate data processor responsibilities demonstrate that they have in place appropriate security policy, standards and controls. Such controls must be proportionate to the impact level of the data being processed. Ensuring that it has appropriate technical and organisational measures in place to guard against unauthorised or unlawful processing of the personal data and/or accidental loss, destruction or damage to the personal data, including all measures required by the Data Protection Laws and in particular Article 32 of the GDPR.

Guidance for Completion

Wherever a provider will already have the appropriate documentation to clarify particular questions or entire sections – please include a copy and simply state reference to the applicable page or section of the document in question. Where a specific question or section may not be applicable to the particular offering scrutinised please state N/A and if it is not obviously apparent, succinctly but clearly state why.

Commitment of Completion

Completed by:

Name:

Position:

On behalf of (Company/Organisation):

Telephone No:

Email:

Address

Date:

Signed:

------------------------

# 01 - Data in Transit Protection

**Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption**.

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 1**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-1-data-transit-protection) |
| Please state the specifics of any encryption methods used for data in transit as a part of any solution offering by the provider. This should state exact types/versions. |
|  |
| Data in transit across public networks shall be suitably protected. Please describe all interfaces to your service (to include user, administration and management etc) and how is access controlled and protected? Include details of any solutions which are supported including the use of private networks, dedicated connections (VPNs). |
|  |

# 02 - Asset Protection and Resilience

**Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure**.

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 2**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience) |
| Please categorically state if the contracted provider themselves wholly own and manage the physical hosting environment including any ITC equipment or storage used? If not please ensure that the later Section 08 concerning supply chain security has been clearly populated to indicate any onward providers details. |
|  |
| Please clearly state the geographical locations of all hosting environments to be used to handle Cornwall Council data assets (this is to include any data mirroring or off-site backup techniques.) |
|  |
| Please state any recognised industry standard which the physical hosting environment is accredited to i.e. ISO/IEC 27001. |
|  |
| Please state if anyone other than the providers authorised personnel, have unescorted (physical) access to any hosting environments to be used to handle Cornwall Council assets? |
|  |
| How often are physical access rights reviewed and how do you control and monitor personnel (including third parties) who access any hosting environments to be used to handle Cornwall Council assets? |
|  |
| Please categorically state all mechanisms in place (i.e. swipe, smartcard, biometric, CCTV, alarms) to deter, prevent and alert of any unauthorised physical access. |
|  |
| Is there an up-to-date physical inventory of all items in any hosting environments to be used to handle Cornwall Council assets and how often are equipment audits carried out to monitor for unauthorised equipment removal or arrival/installation? |
|  |
| How often are checks made to ensure that the physical hosting environment complies with appropriate legal and regulatory requirements? |
|  |
| Please provide details of encryption standards applied to data at rest in all locations including back up media or systems? This should state exact types/versions. |
|  |
| Please provide details of your encryption key management process to include implementation to ensure separation of customer data should the system be multi-tenant? |
|  |
| Please state the processes that are in place for secure disposal of information held by the provider once no longer required or requested to be securely deleted by the Council. Specifically state the solution and technique usage of any sanitisation tools. |
|  |
| Once equipment used to deliver the service reaches the end of its useful life, it should be disposed of in a way that does not compromise the security of the service or Council data stored in the service. Specifically:   * All equipment potentially containing Council data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled). * Any components containing sensitive data are sanitised, removed or destroyed as appropriate. * Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.   Please verify this and state where this may be carried out by a third party. |
|  |
| Please provide any supporting documentation to detail and evidence measures in place to ensure that environmental issues do not cause an interruption to service?  This should include but may not be limited to the following considerations:   * Methods used to prevent or protect from fire, flood or other environmental damage * Continuity arrangements for utilities outages or interruption * Temperature and humidity in the data centre * Air-conditioning considerations and monitoring   Stand-alone or failover generators in the event of a power failure |
|  |
| If agreed as part of the service - detail policies and procedures for backup. This should include procedures for the management of removable media and methods for securely destroying media no longer required. |
|  |
| Detail all measures in place, including any encryption methods used to protect data backed up from unauthorised access. |
|  |
| In case of disruption to service please advise on the RPO (recovery point objective) and RTO (recovery time objective) or equivalent for services? Detail according to the criticality of the service. Will an annual recovery test be performed? |
|  |
| Are information security activities appropriately addressed in the restoration process? |
|  |
| What are the lines of communication to end customers in the event of a disruption? |
|  |
| Are the roles and responsibilities of teams clearly identified when dealing with a disruption? |
|  |
| Has the provider categorised the priority for recovery, and what would be our relative priority (the end customer) to be restored? Note: this may be a category (HIGH/MED/LOW). |
|  |
| How often does the provider test disaster recovery and business continuity plans? |
|  |

# 03 - Separation of Users

**Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.**

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 3**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-3-separation-between-users) |
| Please describe how customer separation is achieved and maintained? This should make reference to all layers of the solution regardless of whether physical or virtual. |
|  |
| Please verify that regular penetration testing is carried out by appropriately qualified (i.e. CHECK, CREST, Tiger scheme) testers and that part of its scope is to determine whether one consumer can affect the service of another consumer. |
|  |

# 04 - Governance Framework

**The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.**

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 4**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-4-governance-framework) |
| Please verify that as a supplier you have in place an appropriate security governance framework that coordinates and directs the overall approach to the management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.  Good governance may typically provide:   * A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title Chief Security Officer, Chief Information Officer or Chief Technical Officer. * A documented framework for security governance, with policies governing key aspects of information security relating to the service. * Security and information security as part of the service provider’s financial and operational risk reporting mechanisms. * Processes to identify and ensure compliance with applicable legal and regulatory requirements relating to the service. |
|  |
| Where personal data assets may be processed on behalf of the Council. Please clarify that the provider can implement measures at the request of the Council to ensure it meets its obligations as Data Controller in accordance with UK Data Protection legislation. |
|  |
| Where relevant data assets may be held. Please clarify that the provider can implement measures at the request of the Council to ensure it meets its statutory obligations for efficiently processing FOI (Freedom of Information) requests. |
|  |

# 05 - Operational Security

**The service provider should have processes and procedures in place to ensure the operational security of the service.**

|  |
| --- |
| **NCSC Guidelines:** [**Cloud Security Principle 5**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-5-operational-security) |
| Please verify that good configuration and change management processes and procedures are in place.  These should be in alignment with a recognised industry standard such as ITIL and provide confidence that:   * The status, location and configuration of service components (including hardware and software components) are tracked throughout their lifetime within the service. * Changes to the service are assessed for potential security impact. Changes are managed and tracked through to completion. |
|  |
| How are default nodes hardened – what recognised industry guidelines are used? |
|  |
| Specify all controls used to protect against malicious code i.e. Anti-Virus, Endpoint HIPs, Application Whitelisting etc |
|  |
| How are principles of least privilege and segregation of duties followed? How are the accounts with the highest level of privilege authenticated and managed? |
|  |
| Provide high level details of the vulnerability and patch management processes and procedures followed. Copies of full documents may be requested. |
|  |
| Please state categorically that the above patch management process and procedures cover all layers of the solution technologies – i.e. network (infrastructure components, routers and switches, etc), server operating systems, virtualisation software, applications and security subsystems (firewalls, antivirus gateways, intrusion detection systems, etc)? |
|  |
| What changes, if any, are made to administrator privileges and roles to allow for extraordinary access in the event of an emergency? |
|  |
| Are any generic accounts holding high levels of systems access in use? |
|  |

|  |
| --- |
| Please confirm that that the provider has formal processes in place for detecting, identifying, analysing and responding to security incidents. A copy of process documents may be requested. |
|  |
| Please clarify that the provider has suffered no major security incidents in the last five years (if the provider has suffered a major incident, further information will be sought via appropriate channels as to how this was responded to, managed and resolved.) |
|  |
| Please clarify that any incidents which may have either a direct or indirect implication for Cornwall Council assets are to be directly reported to Cornwall Council. Contact details and mechanism for this will be agreed pre-contract. |
|  |
| How can Cornwall Council as the cloud customer report anomalies and security events to the provider? |
|  |
| Can the provider detail what information (which relates directly to Cornwall Council assets) is recorded within audit logs? For what period are such audit log data sets retained? |
|  |
| Is it possible to segment data within audit logs so they can be made available to the end customer and/or law enforcement without compromising other customers and still be admissible in court? |
|  |
| What controls are employed to protect logs from unauthorised access or tampering and what method is used to check and protect the integrity of audit logs? |
|  |
| Effective analysis systems must be in place to identify and prioritise indications of potential malicious activity. Please describe any specific SIEM or Protective Monitoring capability tools the provider may have in place. |
|  |
| Define any remote access working practices in place that may allow access to or impact upon Cornwall Council assets. |
|  |

# 06 - Personnel Security

**Service provider staff should be subject to personnel security screening and security education for their role.**

|  |
| --- |
| **NCSC Guidelines:** [**Cloud Security Principle 6**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-6-personnel-security) |
| Please state the policies and procedures which you have in place when hiring your IT administrators or any others with system access or data processor roles? These should include specific clearance levels as applicable and any standards followed such as BPSS. |
|  |
| Please confirm that practices stated above are consistent across all staff handling Cornwall Council assets |
|  |
| What security education program do you run for all staff? Please state how this is evaluated and assessed and how often it occurs. |
|  |
| Please state how often Security access and privilege reviews are conducted for all IT administrators or others with system access handling Cornwall Council assets. |
|  |
| Please state how it is ensured that all staff have signed and agreed to relevant Information Security policies and procedures? |
|  |
| Please state if staff are professionally trained and certified? |
|  |

# 07 - Secure Development

**Services should be designed and developed to identify and mitigate threats to their security.**

* **Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment.**
* **Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment**

|  |
| --- |
| **NCSC Guideline:** [**Cloud Security Principle 7**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-7-secure-development) |
| Please state that a formal system such as SSDLC is in place. Please state a specific maturity model or blend of best practice standards used. |
|  |
| Software development shall adhere to industry best practice and include security consideration. Please provide details of your software development process, which standards are used, and how this meets such standards (for example OWASP TOP TEN) |
|  |
| Please state if ISO/IEC 27034 or any other recognised security standards have been adopted to support the above objectives? |
|  |

|  |
| --- |
| Is there a staged environment to reduce risk, e.g. development, test and operational environments? If so how are these separated? |
|  |
| Please provide details of third party security testing regimes and schedules. Such testing should be conducted on a regular basis by suitably qualified testers and be appropriately scoped to cover attack methodologies which may reasonably be observed in operation. Please provide the most recent PEN test report and details of the scope of works conducted. |
|  |

# 08 - Supply Chain Security

**The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.**

A solutions provider contracted with the Council may in turn incorporate the services of other suppliers as a part of their overall offering. Whilst appearing as a single solution it becomes possible that a number of data processors could be acting together to deliver content or services which involve the processing of personal for which the Council is still the Data Controller.

The primary service provider to the Council must therefore assure that:

* Procurement processes place security requirements on onward third party suppliers and delivery partners.
* The primary service provider manages security risks from onward third party suppliers and delivery partners.
* The primary service provider manages the conformance of their suppliers with security requirements.
* The primary service provider verifies that hardware and software used in the service is genuine and has not been tampered with.

It is vital to the accuracy of this information gathering document and any subsequent risk assessment process it informs that any such layered solution clearly identify which provider is responsible for which components in the table(s) below:

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 8**](https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles/supply-chain-security) |
| Name and contact details for onward provider: |
|  |
| Aspect of solution provided or supported by onward provider: |
|  |
| Sections of this document which have been completed by onward service provider: |
|  |
| Current term of contract with onward provider: |
|  |
| Is Council information shared with, or in any way directly accessible by this third party provider? |
|  |
| Did your procurement process clearly define the security requirements expected from the third party provider? If yes how do you manage the third party provider’s conformance to the security requirements? |
|  |
| Do you have a process in place to manage security risks associated with the third party provider? |
|  |

(This table may be copied and completed as many times as necessary to create a complete inventory. It should also be kept up to date with changes in the chain of sub-processors that take place during the course of providing the service.)

# 09 - Secure Consumer Management

**Consumers should be provided with the tools required to help them securely manage their service.**

**All details of this principle should already be sufficiently clarified in the original procurement SOR IA requirements to which this returned document should be aligned. If you wish to add any additional information please do so.**

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 9**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-9-secure-user-management) |
| Please describe the process for accessing audit log information relating to the system, service or solutions, include what information is captured and the retention periods for such logs? |
|  |
| Please provide detail of all security configuration options for the system, service or solution and how these ensure the confidentiality and integrity of data processed? |
|  |

# 10 - Identity and Authentication

**Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.**

**All details of this principle should already be sufficiently clarified in the original procurement SOR IA requirements to which this returned document should be aligned.** **If you wish to add any additional information please do so.**

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 10**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-10-identity-and-authentication) |
| The system, service or platform shall have robust authentication mechanisms in place. Please describe authentication processes that are offered for the solution, system or service. This shall include the options relating to multi factor authentication services. |
|  |
| How are principles of least privilege and segregation of duties enforced? How are the accounts with the highest level of privilege authenticated and managed? |
|  |

# 11 - External Interface Protection

**All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.**

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 11**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-11-external-interface-protection) |
| Please confirm that all network and communications equipment is hardened in alignment with industry best practice. |
|  |
| Do network security products used by the provider (specifically firewalls) have formal certification? If so at which level? |
|  |
| Define the controls used to mitigate DDoS (distributed denial–of-service) attacks. |
|  |
| Please describe all ‘defence in depth’ network controls applied (i.e. deep packet analysis, traffic throttling, packet black-holing, etc) |
|  |
| Do you have defences against ‘internal’ (that is, originating from the cloud providers networks) attacks as well as external (originating from the Internet or customer networks) attacks? |
|  |
| In the case of internet facing systems please describe the architecture in place to separate presentation, business logic; database etc. layers and ensures protection of back end systems and data from front end attack? (diagrams may be securely shared as necessary) |
|  |

# 12 - Secure Service Administration

**The methods used by the service provider’s administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.**

**The security of a cloud service is closely tied to the security of the service provider’s administration systems. Access to service administration systems gives an attacker high levels of privilege and the ability to affect the security of the service. Therefore the design, implementation and management of administration systems should reflect their higher value to an attacker**

|  |
| --- |
| **NCSC Guidance:** [**Cloud Security Principle 12**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-12-secure-service-administration) |
| Please briefly describe controls and models used to support this principle i.e. Dedicated devices on a segregated network, Service management via bastion hosts etc |
|  |
| Please explicitly state that all administration is only carried out from managed, hardened business devices and not personally owned equipment. |
|  |
| Please state the details including grade and cipher suites used for any VPN solutions that may be used to administrate the service. |
|  |

# 13 - Audit Information Provision to Consumers

**Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.**

|  |
| --- |
| **NCSC Guidance:** [**Cloud** **Security Principle 13**](https://www.ncsc.gov.uk/guidance/cloud-security-principle-13-audit-information-users) |
| Does the provider themselves hold ISO/IEC 27001:2013 or any other recognised industry certification? If so what is the exact scope of the certification? |
|  |
| Is the provider agreeable to securely sharing copies of the most recent audit reports pertaining to the stated certification? (If so this may negate the need to complete subsequent sections where the relevant areas may be covered by the audit reports in sufficient detail.) |
|  |
| Does the supplier implement a programme of regular vulnerability scans, security and penetration tests to ensure the effectiveness of the security controls pertaining to the solution provided. The tests must be conducted by a suitably competent third party. |
|  |
| Is the provider agreeable to securely sharing copies of the most recent security tests redacted as necessary? (If so this may negate the need to complete subsequent sections where the relevant areas are covered by the reports in sufficient detail.) |
|  |
| Please list all Information Security & Data Protection related policies held by the provider and state their last revision date (copies may be requested.) |
|  |
| Please state if the provider is in agreement for Cornwall Council or a delegated third party on their behalf to conduct a pre-arranged on-site audit if deemed necessary? |
|  |

# 14 - Secure use of the service by the consumer

**NCSC Guidance:** [Cloud Security Principle 14](https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles/secure-use-of-the-service)

**Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.**

* **The Council must understand any service configuration options available to them and the security implications of choices they make.**
* **The Council must understands the security requirements on their processes, uses, and infrastructure related to the use of the service.**

**The service provider will be expected to reasonably co-operate accordingly to help the Council support this principle.**

\***Platform as a Service PaaS – Specific**

|  |
| --- |
| PaaS solutions will require specific information gathering |

\***Infrastructure as a Service IaaS – Specific**

|  |
| --- |
| IaaS solutions will require specific information gathering |