|  |  |
| --- | --- |
| **IS TO BE COMPLETED BY SUPPLIER** | |
| Company Name: |  |
| Product/Service Name: |  |
| Completed by: |  |
| Position: |  |
| Date: |  |

**Completing the questionnaire:**

* Answer each question with a simple “Yes” if the solution is fully compliant otherwise answer “No”
* Answers must take account of **all systems that hold or process HCC data** as part of the overall service, not just for the primary business function(s). e.g. ancillary or service management tools including those provided by sub-contractors and/or additional service providers
* When answering a question that has multiple (“at least one of”) acceptable approaches please complete the respective section of the **Supplier Supplementary Notes** table to indicate which of the options your solution supports
* Where a question is not believed to be relevant to the solution then answer with “Yes” **and** complete the respective section of the **Supplier Supplementary Notes** table with a brief statement explaining the rationale
* Where a question is answered “No” the solution is not compliant to HCC standards and will therefore be subject to further scrutiny with the likelihood of exclusion from the procurement process. For these questions provide an additional statement explaining the shortfall and any relevant mitigations in the respective section of the **Supplier Supplementary Notes** table

**Note:** Please ensure the above table is fully completed and all the following questions are answered, with respective supplementary notes as required. **Only fully complete questionnaires will be considered**.

| **#** | **Question** | **Fully comply?** |
| --- | --- | --- |
|  | Is all **user** access to the service authenticated and encrypted as follows:  **Authentication** (at least one of):   * Federated authentication (e.g. SAML) * Multi factor authentication   **Encryption** (at least one of):   * TLS 1.2 (or higher) in transit * IPSec in transit | Yes / No |
|  | Is all **high privilege** access to the service (e.g. administration, development, support, content editing) authenticated and encrypted as follows:  **Authentication** (at least one of):   * Federated authentication (e.g. SAML) * Multi factor authentication   **Encryption** (at least one of):   * TLS 1.2 (or higher) in transit * IPSec in transit | Yes / No |
|  | If any integration data flows between HCC and the service, is the connection authenticated and encrypted as follows:  **Authentication** (at least one of):   * Server certificates * Service accounts with complex 32-character passwords   **Encryption** (at least one of):   * TLS 1.2 (or higher) in transit * IPSec in transit   **Note:** If there is no integration data, you should answer “Yes”. | Yes / No |
|  | If any data flows between multiple service provider locations, is the connection authenticated and encrypted as follows:  **Authentication** (at least one of):   * Server certificates * Service accounts with complex 32-character passwords   **Encryption** (at least one of):   * TLS 1.2 (or higher) in transit * IPSec in transit   **Note:** If there is there is no replication between service provider locations, you should answer “Yes”. | Yes / No |
|  | Are controls in place to limit physical access to the service infrastructure to authorised personnel only? | Yes / No |
|  | Is all service provider (and sub-contractor/additional service provider) staff access to the service infrastructure restricted to secure, managed devices only? | Yes / No |
|  | Is all HCC data and backup data protected at rest as follows?  **Online data** (at least one of)**:**   * 256-bit or higher encryption at rest within the service * Held in secure data centres with physical protection certified to ISO27001 (or PCI if storing payment card data)   **Backup data** is encrypted in transit and (at least one of):   * Securely stored off-site and encrypted to 256-bit or higher * Securely stored off-site in a secure location with physical protection certified to ISO27001 (or PCI if storing payment card data) | Yes / No |
|  | Does the service provider follow a documented data sanitisation process to ensure that?   * Data must be erased (or made unreadable) if infrastructure is moved, re-provisioned, or decommissioned. * Data must be erased (or made unreadable) at HCC request * Data must be returned to HCC at the end of the contract and then erased (or made unreadable) from all service provider systems. | Yes / No |
|  | Does your service have the ability to permanently erase data when no longer required in compliance with Article 5 (1)(d) of the UK GDPR? | Yes / No |
|  | Does the service have the capability to permanently erase all personal data about one person (and if necessary multiple people) in compliance with the UK GDPR Article 17 right to erasure? | Yes / No |
|  | Does the proposed service only store and / or process the HCC personal data (as defined by the UK GDPR) within the UK or European Economic Area (EEA)?  **Note:** This includes high privilege access for service provider administration, support and development teams. | Yes / No |
|  | If the service is used by other customers, is separation between HCC and other customers provided through at least one of the following methods?   * Separate instance of the application. * Separation achieved through dedicated hardware or virtualisation technology such as virtual servers, virtual networks, containers etc. * Separate encryption keys for each customer.   **Note:** If this service shares no infrastructure or services with other customers, you should answer “Yes” | Yes / No |
|  | Does the service provider’s approach to policies, procedures and governance apply to the whole service including any sub-contractors/service providers (e.g. data centre hosting)? | Yes / No |
|  | Is the entire scope of the service certified to ISO27001, those aspects provided by the primary service provider as well as those from any sub-contractors/additional service providers?  **Note:** Copies of certificates will need to be provided to HCC at least annually for the duration of the contract. | Yes / No |
|  | If any card payment services are provided, is the service certified to PCI DSS standard?  **Note:** Full documentation of the handling of card data including copies of PCI DSS Attestations of Compliance will need to be provided to HCC at least annually. If there are no card payment services, you should answer “Yes”. | Yes / No |
|  | If the service directly sends and/or receives email on behalf of HCC (i.e. does not use the HCC mail relay) does it comply with the [NCSC standards for GOV.UK email security](https://www.gov.uk/guidance/securing-government-email) to latest recommended levels (not less than TLS 1.2 encryption in transit, 2048 bit DKIM certificate, DMARC setting p=reject, MTA-STS and SPF records configured)?  **Note:** If there is no direct email traffic, you should answer “Yes” | Yes/No |
|  | Does the entire service have automated protective monitoring in place with real-time alerting of potential security events when they happen (e.g. authentication failures, firewalls logs, virus detections, intrusion detection)? | Yes / No |
|  | Will the service provider alert HCC within 24 hours of a security incident or breach? | Yes / No |
|  | Does the service provider follow a documented change control process for the service? | Yes / No |
|  | Are vulnerabilities for the service managed to the following level:   * Monthly vulnerability scan of service. * Critical vulnerabilities fixed within in 14 calendar days. * High or Important vulnerabilities fixed within 30 calendar days. * Medium vulnerabilities fixed within 60 calendar days. | Yes / No |
|  | Is the service penetration tested annually (or more frequently) by a qualified 3rd party and are any highlighted risks addressed as follows:   * Critical or Serious risks fixed within in 14 calendar days. * High or Important risks fixed within 30 calendar days. * Medium risks fixed within 60 calendar days.   **Note:** Tests should include scenarios for external attack, internal attack and the separation between customers (if the service is used by multiple customers). | Yes / No |
|  | Does the service provider (or sub-contractor/additional service provider) monitor the availability and performance of the service at least daily? | Yes / No |
|  | Are background checks carried out all service provider (and sub-contractor/additional service provider) staff with high privilege access to the service (e.g. administration, development, support) to at least one of the following:   * BPSS (or higher, e.g. DBS) for UK companies * Equivalent standard for non-UK companies | Yes / No |
|  | Are all service provider (and sub-contractor/additional service provider) staff educated and informed as follows?   * Acceptable usage policy * Security policy * Safe handling of personal data training * Staff must review policies at least annually | Yes / No |
|  | Can you confirm that your company has the following?   * an individual has been appointed who is responsible for security * an individual has been appointed who is responsible for data protection   **Note:** It is acceptable for the same person to be responsible for security and data protection. | Yes / No |
|  | Can you confirm that your company has the following organisational measures in place?   * segregation of duties exist so that the scope for unauthorised processing of HCC data is reduced * organisational roles and permissions restrict the access of staff who are not authorised to process HCC data | Yes / No |
|  | Does the service provider (and sub-contractors/additional service providers) follow secure development standards as follows?   * Secure development process must be followed * Secure coding standards must reference external guidance (e.g. OWASP, NIST or equivalent) * Coding standards must be reviewed at least annually * Functional testing of all releases or upgrades * Security testing of all releases or upgrades (e.g. vulnerability scan or penetration test) | Yes / No |
|  | Does the service provide separation between production and any non-production environments that exist? | Yes / No |
|  | Will the service provider ensure that no HCC data is used in non-production environments without HCC’s written approval? | Yes / No |
|  | Are all service provider contractual commitments to HCC supported by contractual commitments between the service provider and all sub-contractors/additional service providers for the service? | Yes / No |
|  | Does the service provider monitor the performance and compliance of all sub-contractors/additional service providers every 6 months (or more frequently)? | Yes / No |
|  | Are all high privilege actions on the service logged, time-stamped and retained for 12 months for audit purposes. | Yes / No |
|  | Are all service security / audit logs retained and protect against unauthorised access or alteration for the following period?   * 12 months in total * At least 3 months readily available (the remaining months from backup or archive) | Yes / No |
|  | Does the service provider (and any sub-contractors/additional service providers with access to HCC data) have a documented process for handling data access requests as follows:   * Requests from 3rd parties will, where legally possible, require HCC approval before information is disclosed * Requests from HCC must be authenticated and authorised before information is disclosed. | Yes / No |

**Supplier Supplementary Notes**

With respect to answers provided above, use the following table to:

* Indicate which of the listed options your solution supports where a question requires “at least one of”
* Identify a question that you believe to be non-applicable **and** provide a brief statement explaining your rationale
* Provide a statement explaining the shortfall and relevant mitigations for any question where you have responded “No” (thereby indicating your service is not compliant with the HCC standard)

|  |  |  |
| --- | --- | --- |
| **#** | **Supplementary Note** | |
|  | **Authentication** - Federated authentication (e.g. SAML) | Yes / No |
| **Authentication** - Multi factor authentication | Yes / No |
| **Encryption** - TLS 1.2 (or higher) in transit | Yes / No |
| **Encryption** - IPSec in transit | Yes / No |
|  | |
|  | **Authentication** - Federated authentication (e.g. SAML) | Yes / No |
| **Authentication** - Multi factor authentication | Yes / No |
| **Encryption** - TLS 1.2 (or higher) in transit | Yes / No |
| **Encryption** - IPSec in transit | Yes / No |
|  | |
|  | **Authentication** - Server certificates | Yes / No |
| **Authentication** - Service accounts with complex 32-character passwords | Yes / No |
| **Encryption** - TLS 1.2 (or higher) in transit | Yes / No |
| **Encryption** - IPSec in transit | Yes / No |
|  | |
|  | **Authentication** - Server certificates | Yes / No |
| **Authentication** - Service accounts with complex 32-character passwords | Yes / No |
| **Encryption** - TLS 1.2 (or higher) in transit | Yes / No |
| **Encryption** - IPSec in transit | Yes / No |
|  | |
|  |  | |
|  |  | |
|  | **Online data** - 256-bit or higher encryption at rest within the service | Yes / No |
| **Online data** - Held in secure data centres with physical protection certified to ISO27001 (or PCI if storing payment card data) | Yes / No |
| **Backup data** - Securely stored off-site and encrypted to 256-bit or higher | Yes / No |
| **Backup data** - Securely stored off-site in a secure location with physical protection certified to ISO27001 (or PCI if storing payment card data) | Yes / No |
|  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  | Separate instance of the application | Yes / No |
| Separation achieved through dedicated hardware or virtualisation technology (e.g. virtual servers, virtual networks, containers) | Yes / No |
| Separate encryption keys for each customer | Yes / No |
|  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  | BPSS (or higher, e.g. DBS) Background Checks (UK companies) | Yes / No |
| Equivalent standard (non-UK companies - provide details below) | Yes / No |
|  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |

**Service Compatibility Questions**

Please complete the following questions to confirm the services compatibility with the HCC technical and service landscape. If all aspects of a question cannot be met, answer “No” and provide details of areas of incompatibility along with any mitigations you may wish to propose in the following Supplier Notes box.

| **#** | **Question** | **Fully comply?** |
| --- | --- | --- |
|  | Will the service operate as required in the HCC technical environment consisting of:   * Windows 10 Enterprise end-user compute   + desktop, laptop and hybrid end-user devices   + Microsoft Intune policy management   + Application distribution through Microsoft Store or Company Portal   + Microsoft Office 365 office applications, email and file storage (OneDrive & SharePoint)   + Microsoft Teams collaboration, messaging and telephony services   + Microsoft Edge (preferred) and Google Chrome browser * Authentication and Access   + Hybrid on-premises and Azure Active Directory   + SAML or OAuth federation   + Individual, non-administrative accounts for all users   + Group memberships for access control   + Conditional Access differentiated controls for HCC and personal devices * Corporate Mobile devices   + Android mobile phones and tablets   + Policy controls enforced by Microsoft Intune   + Principle of least access through policy enforcement by Microsoft Intune   + Application installation via Intune or Google Play Store (HCC approved apps) * On-premises Virtualised Server Infrastructure   + Windows Server 2019 (preferred) or 2016 operating system   + Microsoft IIS application server   + Microsoft SQL Server database   + Microsoft Exchange SMTP relay/gateway * SAP Enterprise Resource Planning platform * No Java based applications on any HCC hosted components of a service | Yes / No |
| **Supplier Notes**: | |