Attachment 4
Crown Travel and Venue Service (CTVS)
Data Security Schedule

Section 1 : Data Security Solution Requirements

Crown Travel and Venue Service (CTVS) Security Principles

The Security Principle Control Matrix, Attachment 5, defines the security characteristics of the Service supplied under the CTVS contract. The Supplier shall assert, and evidence compliance, of the Service Supplied under the CTVS contract against the Security Principles. The Security Principle Control Matrix describes the required security outcomes which the service will need to achieve, in order to provide the Contracting Authority with the assurance and confidence that the Security Risk is being appropriately managed.

Handling, Processing and Storage of OFFICAL-SENSITIVE information

Where the Service is going to handle, process and store OFFICIAL- SENSITIVE information, the Contracting Authority requires additional measures to be implemented to secure data of this type throughout the Service Delivery lifecycle. The measures defined herein are in addition to the Supplier delivering a Service where the residual risk associated with the Service Supplied under the CTVS contract is acceptable to the Contracting Authority. For a Supplier service to handle OFFICIAL-SENSITIVE data the residual risk associated with the additional measures defined below shall be considered acceptable to the Contracting Authority. The additional measures have been cross referenced to the relevant Security Principle headline defined within Appendix A Security Principle Matrix.

Serial	Security Principle Headline	Additional Measures
1.	2. Asset Protection and Resilience	The Supplier shall provide evidence that the infrastructure devices storing any bulk customer data shall not be directly accessible from a device hosted on the internet. In addition, the devices storing bulk data shall be located in the UK. Management and support functions may be off-shored as long as independently assured evidence can be provided that no access to user/consumer information can be obtained from off-shore locations.
2.	4. Governance	The Supplier shall provide evidence of robust handling processes throughout the lifecycle of all information held on the system which conforms to the definition of personal data defined within the Data Protection Act 1998. The robust handling procedures will need to specify the procedural measures implemented to ensure: • There are clearly defined roles associated with any access to bulk customer data. • Where a role is identified as having access to bulk customer data there shall be defined responsibilities

		which detail any actions which can be performed in support of maintaining Service availability. • There shall be a process defined which authorises Supplier staff to be able access to bulk customer data for purposes of delivering and maintaining the Service availability. • Any individual being given access to bulk customer data is aware of the HMG requirements for data protection. • The Supplier nominates an individual within its organisation who is independent from the programme delivery team and is responsible for ensuring the enforcement of the measures defined above.

Section 2: Data Security Delivery Requirements

Data Security Management Support Activities

The Supplier shall also undertake the following activities to support the delivery a secure CTVS Service:

- Secretariat support and hosting of the CSWG. This shall include:
  - Providing facilities to host the meeting
  - Issue agenda and any background papers prior to meeting
  - Issue minutes of meeting
- Presentation of IA risks to the CTVS Programme Board.
- Security support to the Service consumers during take on and Service Delivery. This shall include providing both technical and managerial support to Departmental Service consumers as directed by the Contracting Authority.
- Technical Support to Contracting Authority led Security design reviews, as required. This shall include the production and agreement, with the Contracting Authority's Security Assurance lead stakeholder, of minutes/actions arising.
- Support to risk escalation, as required, in service consuming Departments. This shall include the production and agreement, with the Contracting Authority's Security Assurance lead stakeholder, of a security case.
- Support to Contracting Authority's security risks management actions, this may including (but not limited to):
  - changes to the service implementation,
  - audits of service deliver,
  - changes to the data security documentation

Security Audit

The Contracting Authority shall have the right to audit any evidence produced in support of claimed compliance with any Security Principle.

Security Documentation

The Crown Travel and Venue Service (CTVS) shall produce and maintain the following Data Security documentation in support of the contracting authority's security risk management decision to consume the services:

- Data Security Context - The purpose of this document is to enable the Supplier to complete and maintain a record throughout the lifetime of the Crown Travel & Venue Services Contract, to document the technical implementation context against which the Supplier shall state compliance with the Contracting Authority's Data Security principles. The document shall provide a breakdown of the Service Implementation which includes:
    - Description of each different type of User
    - Description of the Information Exchange with each external entity from both a service implementation and management perspective
    - Provide a breakdown of the key technical aspects of the Service implementation to a level that shall enable the authority to assure comprehensive and consistent application coverage of the principles across the solution.
- Data Security Compliance Statement – The purpose of this document is to enable the Supplier to complete and maintain a record throughout the lifetime of the Crown Travel & Venue Services Contract, to describe the security aspects of their service offering and to provide evidence in support of assurance of their security controls.
- Data Security Risk Register – The purpose of this document is enable the Supplier to complete and maintain a record throughout the lifetime of the Crown Travel & Venue Services Contract, the security risks associated with the solution. For each risk the supplier shall provide the following information
    - an assessment of the severity of the risk
    - description of the remediation action
    - target date for remediation
- Data Security Residual Risk Statement – The purpose of this document is to enable the Supplier to complete and maintain a record throughout the lifetime of the Crown Travel & Venue Services Contract to describe the Residual Security Risks associated with Service Implementation.

HMG Security Risk Acceptance Decision

The Supplier shall have obtained the agreement of the Contracting Authority to accept the residual security risk associated with the Crown Travel and Venue Services (CTVS) service within 12 months

from contract commencement date. In support of the risk management decision the Supplier shall provide the Contracting Authority with a Data Security Residual Risk Statement.

If the Crown Travel and Venue Services (CTVS) **supplier** fails to mitigate the risk to a level that is acceptable to the Contracting Authority, within the first 12 months from contract commencement date, then **the** Supplier shall make **a compensation payment of £10,000 to the Contracting Authority** in recognition of the transfer of risk **to the Contracting Authority.**

If the Contracting Authority is willing to **accept** the residual data security risks then it shall issue a Residual Risk Acceptance Certificate which shall describe the conditions under which the Service can be delivered to HMG consumers. The certificate shall also define the conditions against which the Contracting Authority reserves the right to reassess the decision to manage the residual security risks. If the Contracting Authority wishes to reassess the risk management decision the Supplier shall re-issue the Security Residual Risk Statement.

Data Security Offshoring Approval

Where part or all of the Crown Travel and Venue Services (CTVS) are not delivered from;

- country within the EEA,
- country where the European Commission has made a positive findings of adequacy or
- supplier who has Safe Harbour approval

The Crown Travel and Venue Services (CTVS) Providers shall obtain approval from GSIRO through the Contracting Authority for the off-shored elements. However, if the Crown Travel and Venue Services (CTVS) Provider needs to exchange the Contracting Authorities information with an off shored third party service provider on an individual travel transactional basis (i.e. with a Hotel) then there is NO requirement to obtain GSIRO approval for this aspect of the service.

The Supplier shall be cognisant of supporting HMG compliance with EU data protection legislation throughout the life of the Crown Travel and Venue Services (CTVS) Contract.

Section 3: Management of Crown Travel and Venue Services (CTVS) Data Security

Crown Travel and Venue Services (CTVS) Security Risk Management Roles

The following are the key Data Security Roles involved in the management of the Information Risk associated with the CTVS Service:

- Supplier IA Auditor - Define minimum competence of person a Supplier can use to assure the security aspects of the Service Delivery should as a minimum be certified as an IA Auditor at Senior Level. The individual shall be responsible for ensuring the security documentation is an accurate reflection of the Supplier's Service Supplied under the CTVS contract.
- Contracting Authority's Security Assurance Lead – The Contracting Authority's nominated Security Assurance Lead shall be provided from the CESG Pan-government Accreditation Team.
- Authority's Accreditation Lead -The Authority's nominated Accreditation Lead shall have delegated authority for accepting a level of Security Risk associated with the solution. The Contracting Authority Accreditation resource shall be provided from the CESG Pan –government Accreditation Team.

- Senior Information Risk Owner – The HMG lead for information risk within HMG. The GSIRO is the HMG focus for the management of information risks at Pan Governmental Level.

Crown Travel and Venue Services (CTVS) Security Working Group

The management group responsible for obtaining the information responsible owners agreement to manage the security risk associated with the Crown Travel and Venue Services (CTVS) is the CTVS Security Working Group (CSWG).

The CSWG is a working group **who** manages the delivery of the IA aspect of the solution. The group meets at least twice a year during the Beta Phase and at least **once** annually during the Live Phase.

The CSWG is chaired by the Contracting Authority's Programme Delivery Manager or a nominated representative and **comprises** the following core members:

- Authority's nominated Security Assurance Lead
- Supplier's IA Auditor
- Supplier's Programme representative.

The group is responsible for the following:

- Monitoring the delivery of the evidence in support of claimed Security Principle compliance.
- Managing and maintain the accuracy of the Data Security Risk Register.
- Agreeing Security Test Requirements as being appropriate to assure principle compliance
- Agreeing a Security Case associated with CTVS delivery to enable presentation to the Authority's Accreditation lead for approval.
- Monitoring Security risk impacting upon the operation of the Crown Travel and Venue Services (CTVS) and
- The requirement for identifying, presenting and escalating data security risks which are is outside of the Accreditor's delegated Risk Management Authority.

HMG Data Security Principles Compliance Definition

The supplier shall provide a compliance statement for each Security Principle using one of the following types:

Serial	Principle Compliance	PC Level	Description
1.	Solution Compliant with Principle (SCP)	PC1	The Supplier asserts there is no residual security risk associated with compliance with a Security Principle.
2.	Supplier Managed (SM)	PC2	The Supplier asserts the security risk associated with compliance with a Security Principle which is

			within the Supplier's Risk Management Authority.
3.	Authority's Security Assurance Managed (ASA)	PC3	The Compliance Statement presented to the Authority is assessed as resulting in a security risk that can be managed by the Security Assurance Lead.
4.	HMG SIRO Managed (HS)	PC4	The Compliance Statement presented to the Authority is assessed as resulting in a security risk that can be managed by the G-SIRO <DN reference>.
5.	Residual Risk is Not Manageable (RRNM)	PC5	The Compliance Statement presented by the Supplier is validated by the Contracting Authority Security Representative as resulting in a security risk which cannot be managed by the HMG SIROs

Security Risk Escalation Requirements

The Supplier shall support the process for escalation and management of risk which is outside of the delegated authority of the Authority's Accreditation authority to accept it. In support of this responsibility the Supplier shall, as directed by the CSWG, present any IA risks to the CTVS Programme Board.

If the CSWG recommends approval of the CTS Residual Risk Statement which is rejected by the Authority's Accreditation, the matter can be escalated to the Head of OG-SIRO via the PSN Connectivity Accreditation Panel (PCAP). Any such escalation shall be presented by the CTVS Security Assurance Lead to the Head of OGSIRO with support from both the Supplier and Accreditor.

Appendix A Crown Travel and Venue Service (CTVS) Security Principles Matrix

	Headline	Principle	Sub-points	Implementation Objectives
1	**Data in transit protection**	OFFICIAL data transiting from a Contracting Body service consumer across untrusted networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected between the Contracting Body's end user devices and the service.
		OFFICIAL data transiting the Supplier's internal networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected internally within the service.
		OFFICIAL data transiting untrusted networks should be adequately protected against tampering and eavesdropping (integrity and confidentiality).		Data in transit is protected between the service and other services (e.g. where APIs are exposed).

2	**Asset protection and resilience**	Contracting Body data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. OFFICIAL data shall be protected to a level which is comparable with that required under UK legislation	Physical location and legal jurisdiction	Service Providers shall ensure that the following information is made available to Contracting Body(s): The geographic locations where Contracting Body data is stored, processed or managed from. The applicable legal jurisdictions that the Service Provider operates within and how it provides comparable controls to those required under UK legislation. Contracting Body(s) shall be informed of any changes to the above.
		OFFICIAL data shall physical protection against unauthorised access, tampering, theft and /or reconfiguration of data processing services.	Datacentre security	Data processing locations used to deliver the service are adequately protected.
		OFFICIAL data when stored on any type of removable media or storage within a service shall not be accessible by local unauthorised parties.	Data at rest protection	The Contracting Body has confidence that removable storage media containing their data is adequately protected from unauthorised access.
		The process of provisioning, migrating and de-provisioning resources shall not result in unauthorised access to the Contracting Body's data.	Data sanitisation - retention period	The Service Provider shall inform Contracting Body(s) how long it will take to securely erase Contracting Body data (including from any back ups) from the Service Offering.

			Data sanitisation - Contracting Body on-boarding and off-boarding	The Service Provider shall securely erase Contracting Body data when components are moved or re-provisioned, upon request by the Contracting Body or when the Contracting Body leaves the service.
		Once equipment used to deliver the service reaches the end of it useful life it should be disposed of in a way that does not compromise the security of the service or Contracting Body's data	Equipment Disposal	All equipment potentially holding Contracting Body data , credentials, or configuration information for the service shall be identified.Storage media which has held Contracting Body data shall be appropriately sanitised or securely destroyed at the end of its lifecycle.Accounts or credentials specific to the redundant equipment are revoked.
		The service shall have the ability to operate normally in the event of failures, incidents or attacks	Physical resilience and availability	The Service Provider shall clearly articulate the availability capabilities and commitments of the service. The service has adequate resiliency measures in place.
3	**Separation between tenants**	Separation should exist between different Contracting Body(s) of a service to prevent a malicious or compromised Contracting Body from affecting the confidentiality, integrity or availability of another Contracting Body of the service.		The Contracting Body should be informed of any other Contracting Body they share the platform or service with Separation between Contracting Body(s) shall be enforced at all points within the service where the service is exposed to Contracting Body(s). One Contracting Body shall not be able to affect the confidentiality, integrity or availability of another Contracting Body.

4	**Governance**	The Service Provider has a security governance framework that co-ordinates and directs the provider's overall approach to the management of ICT systems, services and information.	IA Risk Management Processes	A clearly identified, and named, board representative (or a person with the direct delegated authority of) shall be 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. The Service Provider's security governance framework is formally documented, as are policies governing key aspects of information security relating to the service. Information security is incorporated into the Service Provider's financial and operational risk reporting mechanisms for the service. The Service Provider has defined roles and responsibilities for information security within the service and allocated them to named individuals. This includes a named individual with responsibility for managing the security aspects of the service. The Service Provider has processes in place to identify and ensure compliance with applicable legal and regulatory requirements relating to the service.
		.	IA Organisational Maturity	The Service Provider can demonstrate a sufficient degree of IA Maturity.

5	**Operational security**	The Service Provider has processes and procedures in place to ensure the operational security of the service.	Configuration and change management	The status, location and configuration of service components (including hardware and software components) shall be tracked to ensure they can be effectively managed and remain securely configured. Changes to the service shall be assessed for potential security impact. They shall be managed and tracked through to completion.
			Vulnerability management	Potential new threats, vulnerabilities or exploitation techniques which could affect the service are assessed and corrective action is taken. Relevant sources of information relating to threat, vulnerability and exploitation technique information relevant to the service are monitored by the Service Provider. The severity of threats and vulnerabilities relevant to the service are considered within the context of the service and this information is used to prioritise implementation of mitigations. Known vulnerabilities within the service are tracked until suitable mitigations have been deployed through a suitable change management process. Service Provider timescales for implementing mitigations to vulnerabilities found to be present within the service shall be made available to Contracting Body(s).

	The following timescales are applied as a minimum: 'Critical' vulnerability mitigations deployed within 14 calendar days of a patch becoming available. 'Important' vulnerability mitigations deployed within 30 calendar days of a patch becoming available. 'Other' vulnerability mitigations deployed within 90 calendar days of a patch becoming available. 'Critical', 'Important' and 'Other' are aligned to the following common vulnerability scoring systems: National Vulnerability Database Vulnerability Severity Ratings, 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST) Microsoft's Security Bulletin Severity Rating System ratings 'Critical', 'Important' and the two remaining levels ('Moderate' and 'Low') respectively.

Protective monitoring	The service shall collect data events from all relevant Potential Provider devices to support effective identification that all implementation objectives are operating effectively.There shall be effective automated analysis systems in place, supported by adequately trained staff, which identify and prioritise indications in the data that may be related to malicious activities.The Service Provider shall provide Contracting Body(s) with alerts resulting from protective monitoring which impact the implementation objectives within 24 hours.

-	-		Incident management	A defined process and contact route shall exist for reporting of security incidents by Contracting Body(s) and external entities. A definition of a security incident shall be published for the service and the triggers and timescales for sharing such incidents with service Contracting Body(s). The content and format of security incident notifications for sharing information with Contracting Body(s) shall be published. The Service Provider shall initiate investigations into incidents within five hours.
6	**Personnel security**	Service Provider staff should be subjected to adequate personnel security screening and security education for their role.	Service Contracting Body	Service Provider staff that have logical or physical access to the service shall be subjected to adequate personnel security screening for their role. At a minimum these checks shall include identity, unspent criminal convictions, and right to work checks.

7	**Secure development**	Services should be designed and developed to identify and mitigate threats to their security.		The Service Provider shall have a process in place to review new and evolving threats regularly and have development plans in place to progressively improve and reinforce the security of their service against these threats. Software development is carried out in line with industry good practice. Configuration management processes are in place to ensure the integrity of the components of any software.
8	**Supply chain security**	The Service Provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to deliver.		The Service Provider shall clearly define information is shared with or accessible by its third party Potential Providers (and their supply chains). The Service Provider's procurement processes shall ensure that the minimum relevant security requirements for all third party Potential Providers and delivery partners are explicitly documented. The risks to the Service Provider from Supply Chain Potential Providers and delivery partners shall be regularly assessed and appropriate security controls implemented.

				The Service Provider shall monitor its Supply Chain Potential Provider's compliance with security requirements and initiate remedial action where necessary. The Service Provider's procurement process shall ensure that following contract termination all assets are returned, removed (or appropriately destroyed) and any Supply Chain Providers access rights to the Service Provider's internal systems or information are removed. The Service Provider shall categorise each Supply Chain Provider as one of the following: Type 1 - access to aggregated Contracting Body Consumer data Type 2 – access to limited number (less than 10) individual Contracting Body Consumer records Type 3 – access to only part of an I individual Contracting Body Consumer records Type 4 – no access to Contracting Body Consumer records

9	**Secure Contracting Body management**	The Contracting Body should be provided with tools to enable them to securely manage their service.	Authentication of Contracting Body to management interfaces	Only properly authorised individuals from the Contracting Body organisation can authenticate to, and access management tools for the service. Only authorised individuals from the Contracting Body are able to perform actions affecting the service through support channels
			Separation of Contracting Body within management interfaces	No other Contracting Body Service consumer can access management tools for the service. The contracting shall be able to constrain permissions granted to authorised individuals from the Contracting Body to perform actions affecting the service.
			Secure Contracting Body Service Change Authorisation	A Service Provider support procedures shall identify when a support action is security related (such as altering a user's access permissions, or changing user credentials) and ensure appropriate authorisation is in place for this change.
10	**Identity and Authentication**	Contracting Body User and Service Provider access to all service interfaces should be constrained to authenticated and authorised individuals.		The Service Provider shall implement controls which provide confidence that a user has authorisation to access a specific interface.

11	**External interface protection**	All external interfaces of the service should be identified and have appropriate protections to defend against attacks through them.		The service controls and protects access to elements of the service by Contracting Body(s) and outsiders.
12	**Secure service administration**	The methods used by the Service Provider's administrators to manage the operational service (monitor system health, apply patches, update configuration etc.) should be designed to mitigate any risk of exploitation which could undermine the security of the service.		The networks and devices used to perform administration /management of the service shall be apropriate to protect the Contracting Body's data End user devices used for administration shall be enterprise managed assets and shall be securely configured. CESG's EUD Security Guidance provides recommended good practice for configuration of a range of different end user device platforms which can be used to inform the configuration of these devices.
13	**Audit information for tenants**	Contracting Body(s) should be provided with the audit records they need in order to monitor access to their service and the data held within it.		Audit information shall be retained for a minimum of two years or until the Contracting Body leaves the service. The audit information shall be accessible online for a minimum of six months from the point of event collection. The Service Provider shall make tenants aware of: The audit information that will be provided. The format of the data and the schedule by which it will be provisioned (e.g. on demand, daily etc).

14	**Security use of the Service by the consumer**	Service consumers are clear on their responsibilities when accessing the service.		The Service Consumer understands any service configuration options available to them and the security implications The Service consumer understands the security requirements on their processes, uses and infrastructure related to use of the service. The Contract Body is able to educate its privileged users in how to use it safely and securely.