|  |  |
| --- | --- |
| [Arena Home](https://arena.wwf.org.uk/display/ARENAHOME) | **Supplier Security Assessment** |

|  |  |
| --- | --- |
| **Supplier Details** | |
| Supplier/Company Name |  |
| Registered Address |  |
| Name & job title of author |  |
| Services being provided  *(Ensure to enter as much detail as possible, as risk assessment will be based on the information provided.)* |  |

The following questions are to be responded to by the prospective supplier in regards internal systems, processes, resources etc in the context of the services provided to WWF-UK.

**Governance Framework**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| If the service conforms, and has been validated against, a recognised security standard that includes the need for **governance**, provide details of the scope of the assessment with supporting certification: |  |
| If not, confirm, and provide evidence for, the following:   1. 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: 2. A documented framework for security governance, with policies governing key aspects of information security relevant to the service: 3. Security and information security are part of the service provider’s financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk: 4. Processes to identify and ensure compliance with applicable legal and regulatory requirements: |  |

**Personnel Security**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Provide details of the level of security screening conducted on service provider staff with access to our information, or with the ability to affect our service: |  |

**Asset Protection and Resilience**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Detail in which countries our data will be stored, processed and managed: |  |
| Describe your approach to data centre security – if in line with a recognised standard please provide details of such: |  |
| Describe your approach to protecting storage media containing our data – if in line with a recognised standard please provide details of such: |  |
| Describe your approach to data sanitation when requested, released and/or no longer required: |  |
| Describe your approach to equipment disposal – if in line with a recognised standard please provide details of such: |  |
| Provide details of your service availability commitments and ability to recover from outages (eg backup, Business Continuity and Disaster Recovery processes), along with any historical evidence of such: |  |

**Operational Security**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| If the service conforms, and has been validated against, a recognised security standard which covers the need for **configuration and change management**, provide details of the scope of the assessment with supporting certification: |  |
| If not, confirm, and provide evidence for the following:   1. The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime: 2. Changes to the service are assessed for potential security impact. Then managed and tracked through to completion: |  |
| If the service conforms, and has been validated against, a recognised security standard which covers the need for **vulnerability management**, provide details of the scope of the assessment with supporting certification: |  |
| If not, confirm, and provide evidence for the following:   1. Potential new threats, vulnerabilities or exploitation techniques which could affect your service are assessed and corrective action is taken: 2. Relevant sources of information relating to threat, vulnerability and exploitation techniques are monitored: 3. The severity of threats and vulnerabilities is considered within the context of the service and this information is used to prioritise the implementation of mitigations: 4. Using a suitable change management process, known vulnerabilities are tracked until mitigations have been deployed: 5. Timescales for implementing mitigations are met: |  |
| If the service conforms, and has been validated against, a recognised security standard which covers the need for **protective monitoring**, provide details of the scope of the assessment with supporting certification: |  |
| If not, confirm, and provide evidence for the following:   1. The service generates adequate audit events to support effective identification of suspicious activity: 2. These events are analysed to identify potential compromises or inappropriate use of your service: 3. The service provider takes prompt and appropriate action to address incidents: |  |
| If the service conforms, and has been validated against, a recognised security standard which covers the need for **incident management**, provide details of the scope of the assessment with supporting certification: |  |
| If not, confirm, and provide evidence for the following:   1. Incident management processes are in place for the service and are actively deployed in response to security incidents: 2. Pre-defined processes are in place for responding to common types of incident and attack: 3. A defined process and contact route exist for reporting of security incidents by consumers and external entities: 4. Security incidents of relevance to us will be reported in acceptable timescales and formats: |  |

**Identity and Authentication**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Describe your approach to identifying and authenticating users of the service: |  |

**Secure User Management**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Confirm the following:   1. The mechanisms by which you would accept management or support requests from us (phone, web portal, email etc.): 2. The authentication method to ensure only authorised individuals from our organisation can use those mechanisms to affect our use of the service: 3. Whether the above is regularly tested and, if so, provide evidence of such: |  |

**Audit Information for Users**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Provide details of any audit information of user access that will be provided to us, describing what, how and when it will be made available, the format of the data and the retention period associated with it: |  |

**Secure Service Administration**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Describe your approach to service administration (eg. Dedicated devices on a segregated network): |  |

**Separation between Users (Public Cloud Service)**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Provide details of how separation between users of the service is achieved: |  |
| Provide details of penetration tests, security reviews and/or engineering approach to ensure security: |  |

**Secure Development**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| If the service conforms, and has been validated against, a recognised security standard which covers **secure development**, provide details of the scope of the assessment with supporting certification: |  |
| If not, confirm, and provide evidence for the following:   1. New and evolving threats are reviewed, and the service improved in line with the: 2. Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment: 3. Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment: |  |

**Data in Transit Protection**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Describe how data in transit is protected between end user device(s) and the service: |  |
| Describe how data in transit is protected internally within the service: |  |
| Describe how data in transit is protected between the service and other services (e.g. where APIs are exposed): |  |

**External Interface Protection**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Confirm, and provide evidence that a regime of continuous testing is in place to ensure any publicly exposed interfaces are secure: |  |

**Supply Chain Security**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| If the service conforms, and has been validated against, a recognised security standard which covers **supply chain security**, provide details of the scope of the assessment with supporting certification: |  |
| If not, confirm, and provide evidence for, the following:   1. How our information is shared with, or accessible to, third party suppliers and their supply chains: 2. How your procurement processes place security requirements on third party suppliers: 3. How you manage security risks from third party suppliers: 4. How you manage the conformance of your suppliers with security requirements: 5. How you verify that hardware and software used in the service is genuine and has not been tampered with: |  |

**Secure Use of the Service**

|  |  |
| --- | --- |
| **Requirement** | **Response** |
| Provide details of any configuration options available to limit access from specific devices ie. those under our control: |  |

Internal Use only:

|  |  |
| --- | --- |
| Information Security Manager: |  |
| Data Protection Officer: |  |

|  |  |
| --- | --- |
| Name & Job Title of person completing this form: |  |
| Signed: |  |
| Date: |  |