The following requirements must be met by the Supplier. They are not product or service specific. Please note that this document does not replace the [Supplier Assurance Questionnaire](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.gov.scot%2Fbinaries%2Fcontent%2Fdocuments%2Fgovscot%2Fpublications%2Fadvice-and-guidance%2F2023%2F12%2Fscottish-public-sector-supplier-cyber-security-guidance-note-2%2Fdocuments%2Fsupplier-assurance-questionnaire-high-risk-profile%2Fsupplier-assurance-questionnaire-high-risk-profile%2Fgovscot%253Adocument%2FSupplier%252BAssurance%252BQuestionnaire%252B-%252BHigh%252BRisk%252BProfile%252B-%252Bv1.2.xlsx&wdOrigin=BROWSELINK) which MUST be completed during the procurement process.

|  |  |  |
| --- | --- | --- |
| **New Business Cyber Requirements** | **Yes** | **No** |
| **Cyber certificates** |  |  |
| * Cyber Essentials (CE+)/ ISO207001 | Yes |  |
| **Control Framework** |  |  |
| * Ability to provide detail on control framework alignment | Yes |  |
| **Data Retention** |  |  |
| * Ability to provide a justification for length of retention and documented procedure on how data is destroyed (Operational requirements will determine the retention period) | Yes |  |
| **Governance & Risk Management** |  |  |
| * Documented policies and procedures in support of information security for the product/service provided | Yes |  |
| * Internally and externally reporting procedure for cyber security incidents | Yes |  |
| * Risk Management documentation, procedures, accountability and other applicable processes | Yes |  |
| * Implement data protection by design and default – early consideration of data protection risks captured in DPIA | Yes |  |
| **Asset Management** |  |  |
| * Data and information will be processed inside EEA. Provider must provide details otherwise | Yes |  |
| **Supplier Management** |  |  |
| * Appropriate controls and measures to safeguard data (e.g. software, hardware, servers, comms rooms and data centres) | Yes |  |
| * Can demonstrate all 3rd party involvement in the delivery is risk managed, has appropriate assurances and data sharing agreements to mitigate cyber security risks | Yes |  |
| **Access Management** |  |  |
| * Documented process on authentication, privileged access and accounts and user management procedures | Yes |  |
| * Joiners and leavers access management procedure/policy | Yes |  |
| * Multi-factor authentication and SSO exists | Yes |  |
| * Appropriate work from home policy | Yes |  |
| * Documented password policy, embedded within training | Yes |  |
| **Device Management** |  |  |
| * Appropriate network access controls, including revoking access procedures | Yes |  |

|  |  |  |
| --- | --- | --- |
| **Data Security** |  |  |
| * Data is protected using current, proportionate products and standards (including a policy/procedure to reflect) | Yes |  |
| * Information classification policy | Yes |  |
| **System Security – Secure Design & Configuration** |  |  |
| * Documented network segregation and firewall controls | Yes |  |
| * Relevant audits on all system security | Yes |  |
| * Software installation and file download controls | Yes |  |
| **Secure Management** |  |  |
| * Anti-malware capability, policy and procedure | Yes |  |
| **Vulnerability Management** |  |  |
| * Vulnerability scanning and reporting capability with the ability to respond | Yes |  |
| * Can demonstrate up to date practises on monitoring of threats, vulnerabilities and exploitation techniques. | Yes |  |
| * Devices, servers and appliances must be kept up to date. Provide appropriate patching timescales. | Yes |  |
| * Penetration Testing timeframes and accessible reports | Yes |  |
| **Resilience Networks and Systems** |  |  |
| * Documented and tested Disaster Recovery Plan | Yes |  |
| * Documented and tested Business Continuity Plan | Yes |  |
| * Data back-up policy | Yes |  |
| **Self-Awareness & Training** |  |  |
| * Confirmation of staff Information security training and awareness | Yes |  |
| **Detecting Security Events** |  |  |
| * Event logging system of incidents, monitored, assign, prioritised, actioned and with the ability to respond | Yes |  |
| **Minimising the impact of security Incidents** |  |  |
| * Incident management policy including clearly defined roles and responsibilities | Yes |  |
| * Policies and procedures to collect evidence and report incidents to the appropriate authorities | Yes |  |