|  |
| --- |
|  |
| OCSIA Cyber Security Assessment  [Name of supplier being reviewed] |
|  |
| [Name of assessor]  10 November 2020 |
|  |
|  |

|  |
| --- |
|  |

| Section | Description | Response |
| --- | --- | --- |
| Roles & Responsibilities | Has your organisation formally appointed a central point of contact for security coordination? If so, whom, and what is their position within the organisation?  Are responsibilities clearly documented?  e.g. job descriptions, information security policy |  |
| External Parties | Do you work with third parties, such as IT service providers, that have access to your sensitive information?  Does your organization have Business Associate and / or Non-Disclosure agreements in place with these third parties?  If not, what controls does your organisation have in place to monitor and assess third parties?  e.g. Logging of VPN connections, Access logs, etc. |  |
| Information Security Policy & Procedures | Do you have documented information security policies and procedures?  Do you have a formal information classification procedure? Please describe it. In particular, how would sensitive data be categorised?  e.g. Confidential, Restricted, Internal, Public.  Have formal acceptable use rules been established for assets?  Example assets include data assets, computer equipment, communications equipment, etc.  Do you have formal processes in place for security policy maintenance and deviation? |  |
| Risk Assessment | Do you have a process that addresses: the identification and measurement of potential risks, mitigating controls (measures taken to reduce risk), and the acceptance or transfer (Insurance policies, warranties for example) of the remaining (residual) risk after mitigation steps have been applied? |  |
| Compliance with Legal Requirements & data protection | Are processes/policies in place to comply with local, national or international laws and regulations with IT security implications?  eg Data protection, regulatory notification requirements, etc.  Where is data stored? (Country/Region)  Do you replicate data to an alternate/recovery location/region?  Is data storage GDPR compliant?  Is data encrypted at rest and in transit using appropriate cyphers? |  |
| During Employment – Training, Education & Awareness | Have your employees been provided formal information security training?  How are policies been communicated to your employees?  Are periodic security reminders provided?  e.g. New employee orientation, annual training, posters in public areas, email reminders, etc. |  |
| Background Checks | Does your organisation perform background checks to examine and assess an employee or contractor’s work and criminal history? Are particular sensitive positions subject to periodic follow-up background checks?  e.g. Credential verification, criminal history, credit history and references |  |
| Prior to Employment - Terms and Conditions of Employment | Are your employees required to sign a non-disclosure agreement?  e.g. Are staff required to sign a non-disclosure and/or confidentiality form at initial employment |  |
| Termination or Change in Employment | Do you have a formal process to manage the termination and or transfer of employees?  e.g. All equipment is returned, user ID's disabled in systems, Windows, badges and/or keys returned. On Transfer is existing access reviewed for relevance? |  |
| Secure Areas | Provide detail of physical access control methods to prevent unauthorized access to facilities (such as door locks, RFID cards/fobs, other access controls).  Are procedures in place to mitigate key-person dependancies?  e.g. what if the person with the key to the server room is sick?  How are physical access controls authorised and audited (Are policies and procedures in place)?  Are there policies and procedures required for documenting repairs and modifications to physical components of the facility that are related to security? |  |
| Application and Information Access Control - Sensitive System Isolation | Has your IT vendor provided information regarding how your sensitive data system(s) is protected?  Are systems and networks isolated or segregated logicaly and/or topologically based on function?  Are systems processing, transferring or storing sensitive data kept separate?  Are internal (private) and external (public or 3rd party) networks protected?  If so, how? Network or software firewalls, IPS/IDS, Network Access Controls, user access controls. |  |
| Encryption of shared sensitive data | Is sensitive information transferred to external recipients? If so, how is this achieved?e.g. Secure VPN connection with third parties, and/or IT vendors, email, USB stick. Etc. Are controls in place to protect sensitive information when transferred such as encryption?  Are your Internet facing websites protected by SSL encryption? If yes, which versions of TLS are supported? |  |
| Vulnerability Assessment and Remediation | How often do you perform periodic vulnerability scans on your information technology systems, networks and supporting security systems?  e.g. Internal assessments, third party assessments, automated?  What is the security patch management cadence to address vulnerabilities identified?  What security improvements have been made in the previous year? |  |
| Monitoring | Are third party connections to your network monitored and reviewed to confirm only authorised access and appropriate usage?  e.g. VPN logs, server Event Logs, system, application and data access logging, automated alerts, regular review of logs or reports. |  |
| Identity & Access Management | Do you have a formal access authorisation process based on 'least privilege' (employees are granted the least amount of access possible in order to perform their assigned duties) and need to know (access permissions are granted based upon the legitimate business need of the user to access the information) ?  e.g. Role-based permissions, limited access based on specific responsibilities, network access request form?  How are systems and applications configured to restrict access only to authorised individuals?  e.g. Use of unique ID's and passwords.  Do you enforce minimum password length, complexity, history, lockouts, password changes?  Is there a list maintained of authorised users with access (administrative access) to operating systems?  e.g. Active Directory user lists, within sensitive application, Excel spreadsheet of users, HR file?  Do you have a BYOD policy that staff are required to agree to?  Is sensitive information (e.g., opportunities and sales contracts) removed from, or encrypted within, documents and or websites before it is distributed?  e.g. de-identifying of sensitive information prior to being distributed.  Is software installation restricted for desktops, laptops and servers?  Do workstations and servers automatically logoff/lock after a period of inactivity?  Is access to source application code restricted? If so, how? |  |
| Identity Management | Are user IDs for your system uniquely identifiable?  Any shared accounts at all?  e.g. hard coded into applications, someone is sick or unavailable, emergency access to sensitive information? |  |
| Entitlement Reviews | Do you have a process to review user accounts and related access?  e.g. manual process of reviewing system accounts to user accounts in AD for both users and privileged access (such as admins and developers)? |  |
| Antivirus | Has centrally managed antivirus/antimalware software been deployed and installed on your workstations and supporting systems  e.g. desktops, servers and gateways? |  |
| Network defence and Host intrusion prevention systems. | Do you have any host-based IPS for critical systems, next generation firewall with IPS, web application firewalls, web security gateway? To provide layered defence. |  |
| Security Monitoring | Are systems and networks monitored for security events? If so, please describe this monitoring.  e.g. server and networking equipment logs monitored regularly. Servers, routers, switches, wireless AP's. |  |
| Media Handling | Do procedures exist to protect documents, computer media (such as tapes, disks, CD-ROMs, etc.), from unauthorised disclosure, modification, removal, and destruction?  Is sensitive data encrypted when stored on laptop, desktop and server hard drives, flash drives, backup tapes, etc.?  e.g. Data at Rest - Is data encrypted on the server? Backups? Mobile devices? SD Cards? |  |
| Secure Disposal | Are there security procedures for the decommissioning (replacement) of IT equipment and IT storage devices which contain or process sensitive information?  e.g. use of secure wiping – to recognised industry standard |  |
| Segregation of Computing Environment | Are development, test and production environments separated from operational IT environments to protect production (actively used) applications from inadvertent changes or disruption? |  |
| Segregation of Duties | Are duties separated, where appropriate, to reduce the opportunity for unauthorised modification, unintentional modification or misuse of the organisation's IT assets?  e.g. front desk duties separated from accounting. Data analysts access from IT support etc. |  |
| Change Management | Do formal change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerabilities (such as OS or software patching and antivirus/malware updates?  e.g. Changes to the workstations, servers & other systems? Is there appropriate testing, notification, and approval? |  |
| Incident Response | How do you identify, respond to and mitigate suspected or known security incidents?e.g. Incident Form filled out as a response to an incident During the investigation of a security incident, is evidence properly collected and maintained?  e.g. Chain of custody and other computer forensic methodologies followed by internal and/or external parties?  Are incidents identified, investigated, and reported according to applicable legal requirements?  How are incidents escalated and communicated?  e.g. documented process for escalation to management and even outside authorities. |  |
| Disaster Recovery Plan & Backups | Do you have a mechanism to back up critical IT systems and sensitive data?  e.g. nightly, weekly, quarterly backups? Taken offsite?  Have you had to restore files after a systems outage?  Does a Disaster Recovery plan exist for the organisation and does it consider interruption to, or failure of, critical IT systems?  Are disaster recovery plans updated at least annually?  If not, has the backup and restoration process been tested?  What systems are not protected by the Business Continuity Plan?  How many hours of unscheduled downtime have you experienced in the last year?  Are your services covered by DDoS protection? |  |
| Product Security Development Lifecycle | Do you have any product pre-release security threat modelling, secure coding practice, security architecture review and penetration testing? |  |
| Cryptographic materials and key management | Do you have any centralised cryptographic materials and key management infrastructure and program in place to manage centralised key management?  Is PKI (HSM-based or not?) used to issue certs needed for products and cloud service infrastructure? |  |
| Federated Identity Management and Web Services Integration | Describe your SSO and Federated Identity Enablement integration options. E.g. Support for Standards like SAML v2 and OAuth 2.0  Describe your web services and data import/export options.  Provide supporting documentation as required. |  |
| Development | What secure development practices do you follow (e.g. OWASP top 10)?  Are your developers trained on how to protect against SQL injection, XSS, XSRF, Cookie Hijacking and other web based threats?  How are developments security tested? Inhouse by the cyber security manager prior to deployment to production. 3rd party security company at pre-release phase  Is there a “bug bounty”, or responsible disclosure facility?  Do any applications include open source libraries, and if so, how are vulnerabilities in these monitored? |  |
| Security Accrediation | Do you have any security accreditations in place? e.g. Information Security (ISO27001), Quality (ISO9001), PII in Public Clouds (ISO27018), Cyber Essentials Plus  Do you require 3rd party providers to have accreditations in place? |  |
| Contact Information | Whom do we contact if we identify a security issue or breach involving or impacting your product?  Please provide an email address and full contact information |  |
| Service Level Agreement | What is your agreed SLA to respond to initial contact?  What is the agreed SLA to implement changes needed to fix issues according to priority? |  |
| Additional security measures | Does your organization have any additional security measures in place that are not covered by this questionnaire? |  |