Tameside Metropolitan Borough Council

**Tameside Metropolitan Borough Council Cyber Security Assessment Questionnaire**

|  |
| --- |
| S:\cyber.png |

|  |  |  |
| --- | --- | --- |
| Document Title: | Cyber Security Assessment Questionnaire | |
| Version: | 1.0 | |
| Classification: | OFFICIAL - Confidential when Completed | |
| Document Owner: | Digital Tameside | |
| Approved By: | Digital Tameside | |
| Issue Date / Next Revision: | March 2021 | March 2022 |
| Contact: | 0161 342 2962 | |
| Author: | Daniel Ives – Cyber Security Technical Specialist | |

As a valued or prospective supplier to Tameside Metropolitan Borough Council, you play an important role in protecting our information from cyber threats. No one is immune from cyber-attacks so it is paramount that you not only understand the threats but also understand the capabilities your company has in place to protect and guard against such attacks.

For all new or renewals of contacts relating to the procurement of digital IT systems whether hosted externally (cloud based) or on the council’s infrastructure (on premise), it is mandatory for suppliers to complete the following questionnaire in full below and return it to the council’s security operations team.

This form should be completed with honesty and transparency, should there be discrepancies or omissions in the data provided this may preclude you from the procurement process; any existing contracts in place may be subject to termination and the service removed from the council’s digital estate.

Should you require any assistance with completing any part of this questionnaire, you can reach the security operations team in the following ways:

By email: [cybersecurity@tameside.gov.uk](mailto:cybersecurity@tameside.gov.uk)

By telephone: (+44)161 342 3333 and ask for Daniel Ives or a member of the cyber security team.

Please return once completed via email to: [cybersecurity@tameside.gov.uk](mailto:cybersecurity@tameside.gov.uk)

|  |  |  |
| --- | --- | --- |
| Assessment ID: | Reference ID | **FOR TMBC USE ONLY** |

# Company and Project Service Details

|  |  |
| --- | --- |
| Registered Company Name: | Name |

|  |  |
| --- | --- |
| Contact Name: | Name |
| Contact Email: | Email Address |
| Contact Telephone: | Telephone Number |

|  |  |
| --- | --- |
| Individual Completing Form: | Name |
| Job Position | Job Title |
| Form Completion Date: | DD/MM/YYYY |

|  |  |
| --- | --- |
| Name of application or service being provided: | Enter Product or Service Name |

|  |  |
| --- | --- |
| Description of application or service being provided: | Enter Product or Service Description |

|  |  |
| --- | --- |
| System URL (if applicable): | URL |

|  |  |
| --- | --- |
| Contract period: | Contract period |

# Certifications, Processes, Policies and Procedures

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1 Does **your company** maintain any security or other specialized certifications:  These do not include certifications of hosting providers and/or suppliers. | *Please tick all options which apply* | | |
| ISO/IEC 27001 | |  |
| ISO 28000:2007 | |  |
| IASME Governance Standard | |  |
| Cyber Essentials | |  |
| Cyber Essentials Plus | |  |
| PCI DSS | |  |
| Others: | Please specify | |

|  |  |  |
| --- | --- | --- |
| Please provide details on types and certification dates and please provide copies of your most recent reports, audits, or certifications. | *Document or Certification* | *Date Obtained* |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |

|  |  |  |  |
| --- | --- | --- | --- |
| Do all accreditations cover the full company and all its products? | Yes | |  |
| No | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| Do **your suppliers** maintain any security or other specialized certifications?  This includes the service providers your organisation uses e.g. AWS / Microsoft Azure for examples. | *Please tick all options which apply* | | |
| ISO/IEC 27001 | |  |
| ISO 28000:2007 | |  |
| IASME Governance Standard | |  |
| Cyber Essentials | |  |
| Cyber Essentials Plus | |  |
| PCI DSS | |  |
| Others: | Please specify | |

|  |  |  |
| --- | --- | --- |
| Please provide details on types and certification dates and please provide copies of your most recent reports, audits, or certifications. | *Document or Certification* | *Date Obtained* |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |
| Document or Certification Name | DD/MM/YYYY |

|  |  |  |  |
| --- | --- | --- | --- |
| Does your organisation map processes and procedures too standards?  If yes, please select which: | *Please tick all options which apply* | | |
| ISO | |  |
| NIST | |  |
| CIS | |  |
| IASME Governance | |  |
| 10 Steps to Cyber Security | |  |
| NIS Directive Cyber Framework | |  |
| HMG Cyber Security Standard | |  |
| NHS Digital Data Security and Protection Toolkit | |  |
| Other: | Please specify | |

# Technology and Hosting Environment

|  |  |  |  |
| --- | --- | --- | --- |
| The services you run are provided from: | *Please tick all options which apply* | | |
| Not Hosted (Tameside On-premise) | |  |
| Hosted (Company owned Data Centre) | |  |
| Hosted (Shared Data Centre) | |  |
| Cloud Computing services | |  |
| Hybrid Cloud | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| Your disaster recovery is provided from: | *Please tick all options which apply* | | |
| No Disaster Recovery | |  |
| Not Applicable (Tameside On-premise) | |  |
| Hosted (Company owned Data Centre) | |  |
| Hosted (Shared Data Centre) | |  |
| Cloud Computing services | |  |
| Hybrid Cloud | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| If this is a cloud hosted service please state the cloud computing model: | *Please tick all options which apply* | | |
| Infrastructure as a Service (IaaS) | |  |
| Platform as a Service (PaaS) | |  |
| Software as a Service (SaaS) | |  |
| Other: | Please specify | |

|  |  |
| --- | --- |
| If your software or service delivery method is not Tameside On-premise, please state further details of your setup. | Enter Description |

|  |  |
| --- | --- |
| What is the technology stack for the application or service? | Enter Description |

|  |  |  |  |
| --- | --- | --- | --- |
| Are you using Next Generation Firewalls and IPS: | Not Applicable (Tameside On-Premise) | |  |
| Yes | |  |
| No | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| Do you employ application-specific protection, such as Web Application Firewalls: | Not Applicable (Tameside On-Premise) | |  |
| Yes | |  |
| No | |  |
| Other: | Please specify | |

|  |  |
| --- | --- |
| What software development methodologies do you use and how do they incorporate security into the software development lifecycle? | Please specify |

# Identity & Access Management

|  |  |  |  |
| --- | --- | --- | --- |
| How will our users access the application and/or service: | *Please tick all options which apply* | | |
| Username & Password | |  |
| (MFA) Multifactor Authentication | |  |
| X.509 Certificate | |  |
| Active Directory or ADFS | |  |
| Azure AD | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| If MFA is required for our users to access the application and/or service please select the type(s) offered: | *Please tick all options which apply* | | |
| SMS (Text Message) or Voice | |  |
| Email Verification | |  |
| Software OTP | |  |
| Software One-Tap Push Notification | |  |
| U2F FIDO | |  |
| x.509 Client Certificate | |  |
| SAML or OIDC Provider | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| How do your technical support staff access our application and/or service: | *Please tick all options which apply* | | |
| Username & Password | |  |
| (MFA) Multifactor Authentication | |  |
| X.509 Certificate | |  |
| Active Directory or ADFS | |  |
| Azure AD | |  |
| Other: | Please specify | |

|  |  |  |
| --- | --- | --- |
| Can access to the application be restricted by ip address, ip range and or hostname? | Yes |  |
| No |  |

|  |  |
| --- | --- |
| Does the system or service support the use of groups for managing different levels of user access? e.g. standard users, admins etc.? | Enter Description |

# Operational

|  |  |
| --- | --- |
| Describe your disaster recovery (DR) and business continuity practices (BCP) including backup operations for our application and / or service.  How is our data protected for reliability and availability? What are your Recovery Time (RTO) and Recovery Point (RPO) objectives (in hours)? | Please specify |

|  |  |
| --- | --- |
| Describe your incident response processes in relation to beaches and/or cyber-attacks, and client notification of breaches. How and who do you notify when you have a security breach? | Please specify |

|  |  |  |  |
| --- | --- | --- | --- |
| Do you use a SIEM within your organisation? | Yes | |  |
| No | |  |
| Other: | Please specify | |

|  |  |
| --- | --- |
| Do you log all activity and review for malicious activity? If so, how is this done? | Please specify |

|  |  |
| --- | --- |
| What network ports are required for access to this service/application? | Please specify |

|  |  |  |  |
| --- | --- | --- | --- |
| Do you follow a server hardening standard for all systems? | Yes | |  |
| No | |  |
| Other: | Please specify | |

|  |  |
| --- | --- |
| How is vulnerability management handled on your servers? For example, how frequently are servers scanned and patched for operating system and application vulnerabilities? | Please specify |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| What is your software patch frequency and software update release process? | | Please specify | | |
| Who is responsible for backups of the system? | *Please tick all options which apply* | | | |
| The Council | | |  |
| You the vendor | | |  |
| Other: | | Please specify | |

|  |  |
| --- | --- |
| If the council does not manage the backup, please state the backup routines and how long these backups are retained and where these are stored? | Enter Description |

|  |  |  |  |
| --- | --- | --- | --- |
| Who is responsible for patching of the system? | *Please tick all options which apply* | | |
| The Council | |  |
| You the vendor | |  |
| Other: | Please specify | |

|  |  |
| --- | --- |
| If patching of the system is not managed by the council, please state details of any patching / firmware update routines for all components: | Enter Description |

# Data Storage, Classification and Processing

|  |  |  |  |
| --- | --- | --- | --- |
| In the delivery of your service, which type(s) of data are stored in your product/service: | *Please tick all options which apply* | | |
| No Personal Data | |  |
| Personal Data | |  |
| Sensitive Personal Data | |  |
| Criminal Activity | |  |
| Government Data (OFFICIAL) | |  |
| Payment Card Data (PCI DSS) | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| In the delivery of your service, which type(s) of data are processed in your product/service: | *Please tick all options which apply* | | |
| No Personal Data | |  |
| Personal Data | |  |
| Sensitive Personal Data | |  |
| Criminal Activity | |  |
| Government Data (OFFICIAL) | |  |
| Payment Card Data (PCI DSS) | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| In what geographical location is **our data held**: | *Please tick all options which apply* | | |
| UK Mainland (Onshore) | |  |
| European Economic Area (Near Shore) | |  |
| Outside of European Economic Area | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| From what geographical location is, **our data accessed from**: | *Please tick all options which apply* | | |
| UK Mainland (Onshore) | |  |
| European Economic Area (Near Shore) | |  |
| Outside of European Economic Area | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| Which of the following describes the type of access you have to our data: | *Please tick all options which apply* | | |
| None | |  |
| Read Only | |  |
| Update Records | |  |
| Delete Records | |  |
| Generate Records | |  |
| Other (Please specify) | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| Approximately how many of your staff have access to our assets: | Less than 10 | |  |
| Less than 25 | |  |
| More than 25 | |  |
| Other: | Please specify | |

|  |  |  |  |
| --- | --- | --- | --- |
| Is our data encrypted in transit? (e.g. when being sent over a network) | Yes | |  |
| No | |  |
| Other: | Please specify | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Do you use Secure Sockets Layer Security (SSL)?  If yes please select which protocols are enabled: | Yes | | |  |
| No | | |  |
|  | SSL 2.0 | SSL 3.0 | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Do you use Transport Layer Security (TLS):  If yes please select which protocols are enabled: | Yes | | |  | |
| No | | |  | |
| TLS 1.0 | TLS1.1 | TLS1.2 | | TLS 1.3 |

|  |  |  |  |
| --- | --- | --- | --- |
| Which type of SSL/TLS Certificate do you use: | Domain Validated (DV) | |  |
| Organisation Validated (OV) | |  |
| Extended Validation (EV) | |  |
| Other: | Please specify | |

|  |  |
| --- | --- |
| Which certificate authority issues your certificate(s)? | Please specify |

|  |  |  |  |
| --- | --- | --- | --- |
| Is our data encrypted at rest? (e.g. when stored on disk or in a database) | Yes | |  |
| No | |  |
| Other: | Please specify | |

|  |  |
| --- | --- |
| If you are using encryption, at rest, what technologies are used? How are keys stored and secured? Do you use Hardware Security Modules (HSM) for key management? | Please specify |

# Data Disposal

|  |  |
| --- | --- |
| Please explain your Data Disposal process: | Please specify |

# Additional Security Questions

|  |  |  |  |
| --- | --- | --- | --- |
| As part of this service, are there security settings and controls that we the customer are responsible for managing? | Yes | |  |
| No | |  |
| Other: | Please specify | |

|  |  |
| --- | --- |
| Who is responsible for the security aspects of the service or product you provide:  (Please Specify Full Name & Role) | Name & Job Title |