**Attachment 8**

**Information Governance Compliance Audit Checklist**

Please complete the following checklist.

Mandatory requirements are highlighted in **red** and suppliers must meet these as a minimum.

You will be contacted to provide details of the policies and procedures listed below if you have been selected as a successsful bidder.

|  |
| --- |
| **Supplier Name** |
|  |

**Does your organisation have a ICO Data Proctection Registration Number?**

|  |
| --- |
|  |

**Policies**

Please confirm you have the following policies in place:

|  |  |
| --- | --- |
| **Requirement** | **Yes/No** |
| [Information Security Policy (Mandatory requirement)](http://intranet.hounslow.gov.uk/security_policies.htm) |  |
| [Data Protection Policy (Mandatory requirement)](http://intranet.hounslow.gov.uk/data_protection_policy_aug13.pdf) |  |
| Information Security Incident Management Procedure (Mandatory requirement) |  |
| [Password Policy (Mandatory requirement)](http://intranet.hounslow.gov.uk/lbh_password_policy_2_march_2012.pdf) |  |
| User identity and access management Policy (Mandatory requirement) |  |
| [Data Disposal procedure/policy (Mandatory requirement)](http://intranet.hounslow.gov.uk/data_disposal_procedure_may2013.pdf) |  |
| Data Backup policy/procedure (Mandatory requirement) |  |
| Business Continuity and Disaster recovery plan/policy (Mandatory requirement) |  |

Please confirm which of the following additional policies you have in place:

|  |  |
| --- | --- |
| **Requirement** | **Yes/No** |
| [Information Risk Management Policy](http://intranet.hounslow.gov.uk/information_security_risk_policy_oct13.pdf) |  |
| [Records Management Policy](http://intranet.hounslow.gov.uk/records_management_policy.pdf) |  |
| [Freedom of Information Policy](http://intranet.hounslow.gov.uk/foi_policy_nov13.pdf) |  |
| [Acceptable Use Policy](http://intranet.hounslow.gov.uk/lbh_acceptable_usage_policy_2_march_2012.pdf) |  |
| [Internet and Email Policy](http://intranet.hounslow.gov.uk/lbh_internet_and_email_policy_v1-2.pdf) |  |

**IT Security Controls**

Please confirm your IT Security includes the following:

|  |  |
| --- | --- |
| **Requirement** | **Yes/No** |
| Daily Antivirus updates (Mandatory requirement) |  |
| Patch Management (vulnerability) (Mandatory requirement) |  |
| Firewalls (Mandatory requirement) |  |
| User Identification and Authentication (Mandatory requirement) |  |
| Two-factor authentication is used for authenticating users using mobile/remote systems (Mandatory requirement) |  |
| Accredited pen test (Mandatory requirement) |  |
| AES-128/GCM-128 encryption on all devices (Mandatory requirement) |  |

**Personnel**

Please confirm that your staff :

|  |  |
| --- | --- |
| **Requirement** | **Yes/No** |
| Have DBS (CRB) checks carried out prior to commencing employment (Mandatory requirement if supplier handles/process Children's or Vulnerable Adults personal data) |  |
| Aware of their Data Protection and data handling responsibilities (Mandatory requirement) |  |
| Receive annual Data Protection and Information Security Training (Mandatory requirement) |  |

**Internal Audits**

Please confirm that your organisation carry out:

|  |  |
| --- | --- |
| **Requirement** | **Yes/No** |
| Regular audits on compliance with the DPA are carried out (annually at minimum) (Mandatory requirement) |  |
| Regular Information Security audits carried out (annually at minimum) (Mandatory requirement) |  |

**Standards**

Does your organisation adhere to the following standards?

|  |  |
| --- | --- |
| **Requirement** | **Yes/No** |
| ISO:27001/2 Information Security Management standard accreditation (Highly recommended) |  |
| Payment card industry standard PCI-DSS (Mandatory requirement for orgs that take online payments) |  |
| Public Sector Network Code of Connection compliance (Mandatory requirement for Orgs that handle PSN/Central Government, i.e. Housing Benefits, Trading Standards, etc. data)  |  |
| Information Governance Toolkit Compliance (Mandatory requirement for Orgs that work with NHS/Social Care Patient Identifiable Data) |  |