WARRINGTON
Borough Council

# Third Party Information Security

## ICT Third Party Information Security Policy

### 1. INTRODUCTION

1.1 The Council treats its information as a valuable asset and considers that it is essential that information must be protected, together with the systems, equipment and processes which support its use.

1.2 Third party access to Council data, systems and information processing facilities shall be conducted through a robust framework that ensures appropriate controls are in place to restrict access to authorised third party organisations only. Third party access should be managed and compliant to the Council's security requirements in accordance with the Council's information security management system. In order to protect the Council's information appropriately, third party suppliers must implement and maintain the security measures and safeguards appropriate to the nature and use of the information involved in the provision of services.

1.3 Third party suppliers of ICT services to the Council are required to comply, and demonstrate compliance, with the ICT Third Party Information Security Policy.

1.4 Third party suppliers shall designate a named officer who will act as a first point of contact for security issues with the Council. In addition all staff working for the third party supplier, including sub-contractors, with access to the Council's network, systems, data and information shall be made aware of these requirements and shall comply with them as appropriate to their role in the provision of ICT products and services to the Council.

### 2. PURPOSE

2.1 This document sets out the organisational information security measures and requirements that Third Party suppliers of ICT products and services to the Council are required to comply with.

2.2 The policy provides a consistent, flexible and proportionate approach to managing information security risks identified in the provision of ICT products and services to the Council.

### 3. SCOPE

3.1 The scope of this policy applies to a third party supplier that in the provision of ICT products and services to the Council:

3.1.1 will have access to the Council's network, systems or information processing equipment; and/or

3.1.2 will have access to or process the Council's data; and/or

3.1.3 will host the Council's systems and/or store Council data and information.

3.2 This includes, but is not limited to:
- 3.2.1 Third party suppliers involved in the processing of data as defined by the Data Protection Act.
- 3.2.2 Third party suppliers who will access the Council's systems and data from remote locations where the network, information processing equipment and environment are not under the control and management of the Council.

3.3 The policy applies to third party personnel, including employees, contractors, temporary staff, agents and third parties, employed directly or indirectly by the third party for the provision of ICT products and services to the Council.

3.4 If there is any conflict between the security measures and requirements of this policy and the terms of a contract or agreement between the Third Party supplier and the Council, then the terms of the written contract or agreement will take precedence.

## 4. INFORMATION SECURITY

4.1 Third party suppliers of ICT services to the Council are required to ensure that the level of security employed in the provision of ICT services is appropriate to prevent the following:
- 4.1.1 loss of integrity and confidentiality of the Council's data and information;
- 4.1.2 unauthorised access to, use or disclosure of, or interference with the Council's data and information by any person or organisation;
- 4.1.3 unauthorised access to the Council's network, buildings, and tools (including equipment) used by the third party and its sub-contractors;
- 4.1.4 use of the third party access equipment or services by any other third party in order to gain unauthorised access to any computer resource or Council data;
- 4.1.5 loss of availability of the Council's data and information due to any failure or compromise of the third party's products and services; and
- 4.1.6 any and all data loss and data corruption during the provision of the third party's products and services to the Council.

## 5. SECURITY REQUIREMENTS

5.1 Unless agreed with the Council and explicitly stated with an "X" in the 'Not Applicable' column in the table below, the following security requirements shall be applicable to third party suppliers of ICT services to the Council:

| Security Requirement | Not Applicable |
|---|---|
| **SR1. Third Party's Information Security Policy and Management** | |
| SR1.1 A management-approved corporate information security policy or set of information security policies, defining responsibilities and setting out the approach to information security shall be maintained. | |
| SR1.2 Information security policies shall be published and communicated to personnel involved in the provision of services to the Council. | |

| Security Requirement | Not Applicable |
|---|---|
| SR1.3 Information security policies shall have a responsible owner and be maintained, monitored and reviewed on a scheduled basis. | |
| SR1.4 Information security policies shall be reviewed and revised as appropriate in response to a security breach, incident and audit. | |
| SR1.5 Senior management shall provide clear strategic direction and support to assess, monitor and control information security risks, and ensure that information security issues raised are properly addressed. | |
| SR1.6 Designated named individuals or teams shall have responsibility and accountability for all information security policies, implementation and processes. These nominated individuals or teams shall act as the primary points of contact and shall facilitate any security review audit meetings and manage any restoration plan in the event of a security incident, breach or event which affects the availability of the services to the Council. | |
| **SR2. Personnel Security** | |
| SR2.1 Staff recruitment and screening shall be in accordance with Government requirements for pre-employment checks as defined at http://www.cpni.gov.uk/advice/Personnel-security1/Screening/. | |
| SR2.2 Roles and responsibilities relating to the security, processing and interaction of personnel shall be clearly defined, documented and communicated. | |
| SR2.3 Terms and conditions of employment shall define information security requirements, including non-disclosure provisions for employees and contractors. | |
| SR2.4 Personnel including employees, agents, sub-contractors, supplier and other third parties involved in the provision of services to the Council shall have received guidance and be aware of their obligations for information security and the protection of data and information. | |
| SR2.5 Personnel with responsibilities for information security shall have appropriate skills and training support to carry out their role. | |
| **SR3. Supply Chain Management** | |
| SR3.1 Services or any part of services to the Council shall not be sub-contracted without the expressed written permission of the Council. | |

| Security Requirement | Not Applicable |
|---|---|
| SR3.2 Sub-contractors shall, unless explicitly stated otherwise, comply with all the security requirements of this Third Party Information Security Policy.<br>SR3.3 Sub-contractors shall not be allowed access to the Council's network, systems, data and information without an acceptable third party information security risk assessment by the Council.<br>SR3.4 Sub-contractor contracts and agreements shall contain information security, data protection and confidentiality provisions commensurate with the requirements of the Third Party Information Security Policy and any contract with the Council.<br><br>**SR4. Physical Security**<br>SR4.1 Physical work areas that are used in the provision of services to the Council shall be secure to prevent unauthorised access, damage and interference to premises and information. This shall apply, but not be limited, to physical work areas for storage and processing of Council data, systems development, testing, integration and production environments, as well as backup media, printed information and email.<br><br>**SR5. Asset Management**<br>SR5.1 Equipment and devices shall be recorded in a maintained inventory to control and prevent unauthorised network access.<br>SR5.2 Authorised software shall be recorded in a maintained inventory to control and prevent unauthorised installation and execution of software on devices.<br><br>**SR6. Configuration Management**<br>SR6.1 The configurations of hardware and software of mobile devices, laptops, workstations and servers shall be controlled to prevent unauthorised installation and execution of software.<br>SR6.2 Administrative privileges for computers, networks and applications shall be restricted, controlled and managed to prevent unauthorised configuration changes and unauthorised installation and execution of software.<br><br>**SR7. Malware Defence**<br>SR7.1 Anti-virus and anti-malware software and services shall be in place on all hardware to prevent the introduction, creation or propagation of any disruptive element to ICT services, including malicious software. | |

| Security Requirement | Not Applicable |
|---|---|
| SR7.2 Virus and malware protection tools and services deployed shall:<br>▪ be the current and supported version;<br>▪ use definition files and libraries which are updated on a daily basis, as a minimum;<br>▪ provide real-time on-access and on-demand scanning;<br>▪ be able to detect, disinfect, quarantine and delete malware;<br>▪ provide logging, alerts and reporting functionality; and<br>▪ not be able to be disabled, reconfigured or prevented from working by unauthorised users.<br>SR7.3 In event of a virus and/or malware incident affecting the provision of services to the Council, the Third Party shall inform the Council's ICT Service Desk immediately with details of the incident and the measures taken to resolve the incident and prevent reoccurrence.<br><br>**SR8. Secure Network**<br>SR8.1 The configuration and management of networking infrastructure and services shall be designed to prevent unauthorised access and resist security threats and attacks.<br>SR8.2 Vulnerabilities and security weaknesses in the configurations of network devices, such as firewalls, routers and switches, are addressed in a timely manner, commensurate with the threat and in accordance with manufacturer recommendations.<br>SR8.3 Ports, protocols and services on networked devices shall be limited, managed and controlled.<br>SR8.4 The flow of information transferring between networks of different trust levels shall be managed and controlled.<br><br>**SR9. Patch Management**<br>SR9.1 A patch management programme shall be in place that ensures security changes, patches and upgrades in systems, applications and software used in the provision of equipment, services, data processing and/or storage of the Council's data are implemented with minimal delay.<br>SR9.2 Appropriate steps shall be taken to ensure that security changes, patches and upgrades are tested prior to deployment to minimise disruption to the provision of services to the Council.<br><br>**SR10. Security Vulnerability Testing**<br>SR10.1 An established and effective vulnerability assessment process shall be in place that includes assessments of hosts, networks, and applications. | |

| Security Requirement | Not Applicable |
|---|---|
| SR10.2 Remediating vulnerabilities shall be done in a timely manner, commensurate with the threat and in accordance with manufacturer recommendations. | |
| **SR11. Business Continuity and Disaster Recovery** | |
| SR11.1 A Business Continuity and Disaster Recovery Plan shall be in place for the provision of services to the Council. The plan shall set out how services and operations shall be restored following any incident or event considered severe enough to disrupt or cause the failure of business operations. | |
| SR11.2 Testing of Business Continuity and Disaster Recovery plans and capability shall be carried out on a periodic basis in accordance with good industry practice and as agreed with the Council. | |
| **SR12. Location of Services** | |
| SR12.1 Council data shall only be accessed, transferred, stored or processed in the UK. Other locations shall require written approval from the Council subject to an acceptable information security risk assessment. | |
| SR12.2 An information retention and destruction policy shall be in place for services storing Council data to ensure that Council data is not retained for longer than it is needed for business purposes and that it is protected from unauthorised or unlawful processing. | |
| **SR13. Security of Council Data** | |
| SR13.1 Council data and information shall be transferred and exchanged via secure channels. | |
| SR13.2 Council data deemed to contain classified, sensitive or personal data and collected, stored or processed on behalf of the Council shall be encrypted at all times, including whilst at rest, using Council pre-approved encryption algorithms and protocols. | |
| SR13.3 Systems hosting Council data shall perform regular back-ups at scheduled risk-based intervals and at a frequency agreed with the Council. | |
| SR13.4 Testing of system recovery and data restoration capability shall be carried out on a periodic basis in accordance with good industry practice and as agreed with the Council. | |
| SR13.5 Council data stored by a Third Party shall be available in an agreed usable format at the point of service exit and contract termination, at no additional cost to the Council. | |

| Security Requirement | Not Applicable |
|---|---|
| SR13.6 Secure deletion and destruction of Council data shall be performed at the point of service exit and contract termination, at no additional cost to the Council. | |
| **SR14. Secure Remote Access** | |
| SR14.1 Remote access to the Council's network, systems and data shall be subject to an acceptable information security risk assessment. | |
| SR14.2 Remote access to the Council's network, systems and data shall be controlled via a secure gateway that implements strong authentication. | |
| SR14.3 Remote access shall only be enabled for the live delivery of support and maintenance services and will be limited to personnel directly involved in the provision of services to the Council. | |
| SR14.4 Passwords for accessing Council network, systems and data via Council approved and provisioned access methods shall be securely stored and restricted to personnel directly involved in the provision of services to the Council. | |
| **SR15. Secure Application and Systems Development** | |
| SR15.1 Technical standards for information systems, applications and software used in the processing and storing of Council data and information shall be defined, documented and maintained in accordance with good industry practice. | |
| SR15.2 Application and systems development methodologies and processes shall ensure the secure development and acquisition of software, code and systems accessing and processing the Council's data. | |
| SR15.3 Changes to information systems, applications and software involved in the provision of services to the Council shall be subject to security control requirements and tested prior to implementation. | |
| SR15.4 The Council shall be notified of upgrades or configuration changes that impact on the security of information systems, applications and software involved in the provision of services to the Council. | |

| Security Requirement | Not Applicable |
|---|---|
| **SR16. PCI-DSS Compliance**<br>SR16.1 Services to the Council that involve financial transactional functionality shall comply with the latest version of the PCI-DSS and, where applicable, PA-DSS requirements. Evidence of compliance shall be provided through external certification or self-assessment declaration as agreed with the Council.<br>SR16.2 Web-based, hosted or cloud services which process or redirect to a service which processes card payments shall be included in the Council's quarterly vulnerability tests run by third-party Approved Scanning Vendors (ASVs).<br>SR16.3 Vulnerabilities identified shall be actively investigated and resolved within the timescales necessary for the Council to remain PCI-DSS compliant.<br><br>**SR17. Incident Management**<br>SR17.1 A security incident response procedure shall be developed and maintained for the provision of services to the Council.<br>SR17.2 Security incidents and breaches that impact on the Council shall be:<br>▪ Immediately reported to the Council's ICT Service Desk with details of the cause, impact and nature of the Council data involved.<br>▪ Immediately remedied by the Third Party to contain the incident and prevent further occurrences, at no additional cost to the Council.<br>SR17.3 In the event of a security incident and breach the Third Party shall cooperate and comply with the Council's reasonable instructions.<br>SR17.4 As soon as reasonably practicable, and at the request of the Council, a report shall be provided to the Council, to include full details of the security incident with the steps taken to mitigate or resolve them.<br><br>**SR18. Security Audit and Logging**<br>SR18.1 Regular monitoring and testing shall be used to ensure compliance with information security policies and standards.<br>SR18.2 Systems and services used for accessing, processing, storing and/or collecting Council data and information shall be capable of full usage audit, including the audit of administrative functions, with audit logs retained for a period of at least 90 days. | |

## 6. SECURITY TESTING

6.1 The Council employs the Nessus security scanning tool to test software and application vulnerability ensuing that deployed ICT solutions and services are secure and not vulnerable to unauthorised access or threat. On premise based solutions shall be required to successfully complete a Nessus test. Where vulnerabilities are identified the Third party supplier shall work with the Council to remediate the issue(s).

6.2 Third party suppliers shall be responsible for remediating vulnerabilities identified in their software and services, including supporting infrastructure and third party software, in a timely manner and commensurate with the threat as directed by the Council.

6.3 Systems, software and utilities supplied to the Council, including the use of other third party software, shall be the latest supported versions and be able to be upgraded and patched to address security vulnerabilities and weaknesses identified either in security testing undertaken by the Council or in accordance with manufacturer recommendations.

6.4 Third party suppliers shall be responsible to ensure that all components, including other third party components, used or required in the operation of their software, systems and solutions are fully supported versions without any detriment to performance or user operation, unless approved by the Council in writing. This includes upgrading and patching third party supplier's own software, systems and solutions in order to operate on supported versioned components.

## 7. MONITORING AND AUDIT

7.1 The Council shall be able to undertake monitoring of all activity performed by the third party accessing the Council's network in the provision of the services.

7.2 Except where an audit is imposed on the Council by a regulatory body, the Council may either itself or via its nominated independent auditors conduct an audit to review the integrity, confidentiality and security of the Council's data and information.

7.3 The scope of any audit requested by the Council shall be agreed with the third party and shall relate to the services provided by the third party.

7.4 Audits requested by the Council will be in accordance with any contractual requirements between the Council and the third party.

7.5 The Council shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the third party or delay the provision of its services.

7.6 Subject to the Council's obligations of confidentiality, the third party shall, on request, provide the Council or its nominated representatives with all reasonable co-operation and assistance in relation to each audit, including:

7.6.1 all information requested by the Council within the scope of the audit;

7.6.2 reasonable access to any sites controlled by the third party and to any equipment used in the performance of the services; and

7.6.3 access to third party personnel.

7.7 If an audit identifies that the third party has failed to maintain its compliance with the Third Party Information Security Policy, the Council shall agree and implement a remedial plan with the third party.

## 8. THIRD PARTY INFORMATION SECURITY RISK ASSESSMENT

8.1 The Council shall carry out third party information security risk assessments as may reasonably deem necessary in order to review the integrity, confidentiality and security of the Council's data and information.

8.2 Third party information security risk assessments may be undertaken:

8.2.1 on an annual basis;
8.2.2 prior to the renew and/or extension of any contract;
8.2.3 where there has been a change or a request to change the specification and/or provision of third party services;
8.2.4 following a security incident;
8.2.5 on request to change a third party's access requirements and privileges; and
8.2.6 prior to any audit or review of services.

8.3 Subject to the Council's obligations of confidentiality, the third party shall, on request, provide the Council with all reasonable co-operation and assistance in relation to each third party information security risk assessment, including providing information requested by the Council in a timely manner.

8.4 If a third party information security risk assessment identifies that the third party has failed to perform its obligations in respect of the Third Party Information Security Policy, the Council shall agree and implement a remedial plan with the third party.

8.5 Failure to respond to the Council's reasonable request for information to complete a third party information security risk assessment may result in suspension of the third party's access privileges to the Council's Network and the third party will be deemed to be in default of its contractual obligations to the Council.

## 9. CORRECTIVE ACTION

9.1 If a third party fails to provide services in manner that complies with of the Third Party Information Security Policy, the Council will notify the third party in writing:

9.1.1 the precise manner in which the third party is in default;
9.1.2 the action which (in the opinion of the Council) the third party must take to remedy the default;
9.1.3 a reasonable time period (bearing in mind the nature of the default) in which the third party should take the action to remedy the default.

9.2 In the event that the third party fails to provide the services in manner that complies with Third Party Information Security Policy to such an extent that compromises and/or causes the Council to breach the Public Services Network Code of Connection, the Council will not be liable for all or any additional cost and/or expense incurred or to be incurred by the third party in order to perform its contractual obligations to provide the services to the Council.

9.3 The Council shall not be charged for additional cost and/or expense should the Council to maintain its compliance to the Public Services Network Code of Connection not enable the third party to access the Council's network remotely using the third party access equipment and the third party, in order to provide the services, is required to visit the Council's premises and use the Council's information processing facilities and equipment.

## 10. COMPLIANCE

10.1 In the event that the third party fails to provide the services in manner that complies with the Third Party Information Security Policy the Council shall limit the third party's access to the Council's systems, applications, data and information pending clarification and resolution.

10.2 Non-compliance with the Third Party Information Security Policy may lead to the withdrawal of the Council's network and information technology resources to the third party and the cancellation of any contractual agreement with the third party.