Information and Cyber Security Policy for Supply Chain, Partners and Service Providers

Contents

Version Control

Version	Description	Release Date	Issued By
1.0	Initial version for suppliers/partners.	June 2020	Information Security Officer
2.0	Updated CoCo to reflect up to date version	March 2023	Information Security Officer
3.0	Updated ERC SSO requirement from ADFS to Azure AD app registration and enterprise applications.	April 2023	Information Security Officer
4.0	Point 9.3 updated to reflect ICO guidance related to “data protection by design and default”	Oct 2023	Information Security Officer
5.0	Addition of section 14 Artificial Intelligence	Dec 2023	Information Security Officer

1. Introduction and scope

Where you do not, or cannot, comply with any areas of this policy that are relevant to the solution, contractual arrangement or services being provided you must inform the Council immediately and prior to any contractual arrangement. Areas must be maintained for the duration of any contractual arrangement.

1.1 Information plays a critical role in the lives of East Renfrewshire Council (ERC) customers, employees, and business; as a result information systems and physical assets, including supporting processes, systems, networks and equipment, need to be appropriately protected to ensure that the Council can continue to operate and provide its service delivery.

1.2 The Council's supply chain and partners that we share data with, or who provide applications, systems or support, have a responsibility to provide appropriate and continued protection for the full life span of any information shared or application/systems used. This extends to any further authorised sharing undertaken with another party. Suppliers and partners are responsible for ensuring Council requirements are passed down to those parties.

1.3 This policy applies to suppliers and partners providing products and services and presents ERC's policy to ensure appropriate security measures to assure the continued security of our:

- information;
- products or services provided including applications;
- computing systems and networks.

2. Purpose

2.1 The purpose of Information and Cyber Security is to protect the information, and the systems on which they reside, of ERC, our customers, and our employees through the implementation of appropriate policies, standards, processes, and technology.

2.2 This Policy provides the foundations and framework for appropriate and efficient information security as a fundamental aspect of corporate governance.

2.3 This policy applies to all aspects of cyber and information security, including the specification, design, development, installation, operation, connection, use and decommissioning of the systems, services and equipment used to store, process, transmit or receive information.

3. Governance and responsibility

3.1 The Council ensures that suitable frameworks exist to initiate and control the implementation of information and cyber security between itself and external organisations. This Policy provides the basis for this.

3.2 All staff and individuals with access to Council information will appreciate that they have an individual responsibility to ensure that information is handled appropriately. 3rd parties and partners who access council information will be expected to adhere to the requirements of this policy in the way that they work.

3.3 For services provided, the supplier will be responsible for all aspects of security including data: at rest, being processed and in transit. As such the supplier will ensure that they and their supply chain involved in delivery of services for the Council complies with the minimum security requirements as set out and their continued compliance throughout any contractual term.

3.4 This shall cover the entire lifecycle from when information is created through to when it is destroyed irrespective of the format it exists in e.g., electronic, digital, paper, video, voice etc. Any destruction will be in line with time-scales and processes contractually agreed for the service being provided and will be in line with this policy.

4. Policies and Procedures

4.1 The Council ensures that suitable frameworks exist to initiate and control the implementation of information and cyber security between itself and external parties including partners and suppliers.

4.2 Suppliers and services provided are required to align and comply with all elements and controls of Cyber Essentials https://www.cyberessentials.ncsc.gov.uk/. Where suppliers host, process or hold destruction responsibility for personal, special category or business sensitive data they will be Cyber Essentials accredited.

4.3 Suppliers will have policies in place that ensure the continued confidentiality, integrity and availability of Council information and systems. It is acknowledged that some listed below may be incorporated as part of a wider policy however all will be in place:

- IT Security / Information Security;
- Anti-virus and advanced threat protection;
- Patch management;
- Configuration and Change management;
- Transient equipment and transient data management;
- Removable media;
- BYOD ensuring no unmanaged device access to data/systems is achievable and that no unauthorised individual can gain access to data;
- Visitors to premises;
- Backup of data;
- Retention of data;
- Disposal / Reuse of hardware assets;
- Disaster Recovery and Business Continuity;
- Ongoing testing and vulnerability management of internet facing components/web sites.

5. Human resources and training

5.1 All staff involved in delivering services will be trained in security roles, procedures and data protection. Training will extend to the permitted use, handling, processing and further sharing of Council information assets and use of systems.

5.2 Background checks on all permanent, temporary and contracting staff that are accessing information or supporting systems will be undertaken, confirming at the very least, qualifications, identity, right to work in the UK and contacting all referees.

Additional criminal background checks (unspent convictions via disclosure Scotland or equivalent) will be undertaken for staff with general access or administrative access to systems/applications which permits access to information assets defined as personal, sensitive, personal identifiable or special category information under data protection laws.

5.3 Supplier will be able to name all staff who either:

- provide system support with administrative access to systems/applications;
- have ability to gain access to information assets defined as business sensitive, personal, personal sensitive, personal identifiable information or special category under data protection law.

5.4 Supplier remote solutions used to gain access to Council systems or data will be state of the art with access gained from company owned and managed equipment and utilize strong authentication methods ensuring the identification of staff and equipment in use.

5.5 Suppliers requiring access to the ERC computing and network environments will comply with Council conditions of access and be aware that VPN access is managed and not provided 24/7. Requirements for ad-hoc VPN access out with normal office hours will be managed however such access is not guaranteed and on each occasion is subject to an exemption process.

5.6 Supplier will ensure that remote access by their staff is authorised, all staff named and identified and logs of access maintained for a minimum of 6 months. Logs will be available on request by the Council.

5.7 Prior to accounts being created the supplier and their staff will comply with ERC's Code of Connection (example can be located in Appendix 1).

6. Supplier owned/contracted data stores and file locations

6.1 The supplier will be responsible for all aspects of physical, logical, data security and data protection for all hosting and data storage environments. This includes the application of physical and logical controls to restrict access to sites, buildings, data and computer facilities and the management of neighbourhood risks

6.2 Controls will be in place to detect and prevent compromise of data storage environments and data, including user access to that data. The supplier will use both technical and operational controls as assurance such as up-to-date antivirus definitions from an industry-accepted antivirus software seller, EAL4 firewalls, intrusion detection / prevention mechanisms and active reviews of audit logs.

6.3 Data under the remit of data protection laws will be encrypted at rest. Encryption should be FIPS140-2, FIPS140-7, CPA approved or equivalent.

6.4 The supplier will be responsible for ensuring that Council data is securely segregated from data belonging to other organisations by using assured gateway/boundary controls and the internal segregation of Council services from those of other customers.

6.5 All data hosting locations will be independently security tested to ensure continued protection of information assets, credentials and systems with period checks at least yearly.

6.6 All technologies and software used will be maintained to most recent standards with no legacy or compromised versions being used. Any controls scoring between 4.0 and 5.9 CVSS scoring, or equivalent, will be addressed within 2 months. Controls scoring 6.0 or above, or equivalent, will be resolved immediately. Controls not addressed will be reported to the Council with a plan of action for resolution including time scales.

6.7 All systems, operating systems and applications will be patched to vendor's latest versions in line with a published policy with critical patches being applied within 14 days.

6.8 Data is not permitted to be transferred via routes and networks out with the UK or the European Union. Where this may be the case the supplier will inform the Council.

6.9 Where data stores are not within the UK suppliers will inform the Council. Suppliers will provide additional security controls and documentation to the Council's satisfaction before non-UK based data stores are used.

6.10 Formal procedures will exist to ensure that Council data is destroyed and unrecoverable during hardware asset destruction or renewal programs for all hardware, peripherals and data bearing devices used in the delivery or the provision of services.

7. Data in transit and sharing between parties

7.1 Council data in a transient state will be encrypted to levels not subject to known flaws or security issues and be of accepted industry standards. Encryption in use will be maintained to latest patching and security levels.

7.2 Legacy protocols such as SSL, TLS 1.0 and 1.1 will not be used. All internet bound traffic will utilize the latest version of protocols available. Where vulnerabilities become known for protocols in use, the Supplier will advise the Council within 5 working days advising of the suppliers plan for addressing the issue.

7.3 For Cloud based hosted provided solutions, applications and services, suppliers will comply with the 14 principles of the Cyber Security Requirements for Cloud Service providers https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles . and the Government's 10 Steps to security
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
The supplier will inform the Council when principles are not implemented.

7.4 Data sharing between ERC and the supplier will be protected. This will include that located on laptops, tablets, smart devices, USB storage devices, optical media, email in transit, data in transit between 2 points across a network including VPNs and the Internet.

7.5 Where data sharing is undertaken via email all parties will comply with NCSC email security and anti-spoofing guidance in that SPF, DKIM, DMARC and mandated TLS are applied. Encryption should be FIPS140-2, FIPS140-7, CPA approved or of accepted industry standards. Where a supplier cannot achieve email security they will utilize secure email systems available from the Council such as ClearSwift secure mail.

8. Local storing of data

8.1 Where Council data is stored or retained locally on supplier equipment such as office Servers, PC's, laptops, tablets, smart devices, MFD devices, USB storage devices, flash storage, optical media etc. data will be encrypted to levels not subject to known flaws or security issues. Encryption in use will be maintained to latest vendor patching and security levels.

8.2 Access to data will be in line with Section 5.

9. Supplier provided or developed application/system

9.1 "Application/System" covers any occurrence of a system being provided to store, manage, transmit or process credentials, information or data belonging to the Council. For clarity this includes mobile apps, databases and applications where users may or may not provide credentials, or use single sign on, to access and interact with information.

9.2 Suppliers will not spoof any ERC email domain. Where emails will originate from within an application/system this will comply with Council requirements. Where email is an integral component of the solution and requires to traverse the internet all email will comply with NCSC email security and anti-spoofing guidance in that SPF, DKIM, DMARC and mandated TLS are applied.

9.3 Applications will be developed in line with ICO guidance related to "data protection by design and default" to minimise privacy risk and ensure security extends throughout the entire lifecycle of data to ensure cradle to grave protection. The UK ICO requirements can be located at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/

9.4 Applications will encrypt data at rest were information assets can be defined as personal, sensitive, personal identifiable or special category information under data protection laws.

9.5 Access controls will be implemented to achieve data protection and privacy and ensure role based access control to restrict user access to permitted data. Where systems will process information defined as personal, sensitive, personal identifiable or special category information under data protection laws they will have the ability to:

- use MFA for all admin accounts;
- where traversing the internet use MFA for all user accounts;
- utilise secure printing features (i.e. not be dependent on direct IP printing).

9.6 Reporting functionally will relate directly to the access rights of the user undertaking the task therefore ensuring only permitted data is returned under all circumstances.

9.7 Where test environments are being provided these will be separate from live systems, enable the use of test data and support Council compliance with data protection law. Testing facilities will ensure data cannot be compromised by utilising technology to prevent accidental or malicious compromise.

9.8 Applications will be independently security tested to ensure continued protection of information assets, credentials and systems by the undertaking of an initial independent IT Health Check of the application and further checks undertaken as major developments are made.

9.9 All software used will be maintained to most recent standards with no legacy or compromised versions in use. Any controls scoring between 4.0 and 5.9 CVSS scoring, or equivalent, will be addressed within 2 months. Controls scoring 6.0 or above, or equivalent, will be resolved immediately. The supplier will advise ERC where controls are not addressed.

9.10 All application components will be patched to vendor's latest versions in line with a published policy with critical patches being applied within 14 days. This includes all plug in software such as java, flash etc.

9.11 Audit logs will provide at the minimum: UserID's, dates, times, key events such as log on/off, searching for records, reading of records, printing of records, terminal ID, successful and rejected system access attempts, use of privileges, changes to system configuration.

9.12 Audit logs will be tamper proof from all users including admin level accounts.

9.13 Audit logs will be maintained for a minimum of 6 months.

9.14 Passwords for access will allow configuration to use a complex syntax including a combination of letters, numbers and symbols and allow prevention of simple passwords such as dictionary words or known names. All credential passwords will be salted, hashed and encrypted. The Council must be advised of any non-conformance.

9.15 Mobile apps will be unable to operate on jail-broken, rooted, or similar device configurations.

9.16 Sandboxed applications used to gain access to Council systems or data will ensure no ingress or egress from the application to the device and vice versa.

9.17 Cloud hosted solutions will have the ability to use single sign on in with ERC Azure AD app registration and enterprise applications. SSO **must not** have a requirement to link via email address as the Azure AD UPN. This must be configurable to use another syntax/field from Azure AD.

9.18 Cloud hosted solutions will have the ability to support multi factor authentication MFA.

10. Backups and disaster recovery

10.1 Backup and DR data stores will comply with Data Centre requirements under Section 6.

10.2 The supplier will ensure that data residing within Backup and DR data environments is provided the same security, protection and user permitted access as data within live data stores.

10.3 The supplier will maintain backup and DR polices for continued provision of services to the council.

11. Security incident management

11.1 The supplier will have procedures in place for investigating breaches of security.

11.2 The supplier will have a process for informing the Council of any malicious or accidental compromise affecting Council information assets or systems within 1 working day of the event where data or systems may be defined as business sensitive, personal, personal sensitive, personal identifiable or special category data (if additional Council contracts define an earlier time scale that will take precedence).

11.3 Other data sets will be reported within 3 working days (where additional contract terms or framework agreements state earlier timescales those will take precedence).

12. PCI Applications and Services

12.1 Any services, application, process or system that involves the processing of card payments will have accreditation to the applicable standard(s) such as:

- PCI
- PA DSS
- PTS
- QIR

12.2 The supplier will ensure the application has been independently security tested to ensure continued protection of information assets, credentials and systems. This requires an

initial independent IT Health Check testing of the application and further checks to be undertaken as major developments are undertake. Application testing should be undertaken by accredited testers under a scheme such as PCI, CHECK, Tiger, CREST. Testing will include security testing against the requirements of OWASP where applications can be internet facing.

13. Destruction or sanitisation services

Digital Formats

13.1 Suppliers providing digital destruction or sanitisation services are fully responsible for their supply chain, assuring compliance with this policy and providing services that enable ERC to comply with data protection laws.

13.2 For supplier owned digital formats: formal procedures will exist to ensure that Council data is destroyed and unrecoverable during hardware asset destruction or renewal programs for all hardware, peripherals and data bearing devices used in the delivery or the provision of services. The supplier will assure this for their entire supply chain

13.3 For ERC owned removable HDD's (magnetic memory) where the supplier provides a destruction or sanitisation service: where physical data bearing media is not being physically destroyed i.e. by shredding all data bearing media will be erased with certified erasure products (refer to the NCSC list of certified data erasure products).

13.4 For ERC owned solid-state/flash memory storage drives where the supplier provides a destruction or sanitisation service: where physical data bearing media is not being physically destroyed i.e. by shredding all data bearing media will be erased using the manufacturer's erasure tool. Where such a tool does not exist all occurrences of steps taken to sanitation the data storage will be discussed and agreed with ERC.

13.5 For ERC owned flash based media where the supplier provides a destruction service. Where physical data bearing media is being physically destroyed i.e. by shredding this will produce particles no greater than 6mm. This would include USB thumb drives, SD/microSD cards or flash chips.

13.6 All destruction processes for ERC owned medium will provide a full audit trail of equipment inventory, journey taken, storage locations, duration of storage prior to processing, destruction or sanitisation process and a destruction/sanitation assurance certificate returned to ERC.

Paper Formats

13.7 Suppliers providing paper destruction services are fully responsible for their supply chain assuring compliance with this policy and providing services that enable ERC to comply with data protection laws.

13.8 Suppliers will have achieved accreditation with ISO9001 incorporating EN15713.

13.9 Shredding, when undertaken, will as a minimum comply with DIN 66399 security Level 4 (160mm2). Where paper is pulped or burned shredding is not necessary.

13.10 Destruction processes will provide a full audit trail of paper inventory, journey taken, storage locations, duration of storage prior to processing, destruction process and a destruction assurance certificate returned to ERC.

14. Artificial Intelligence

This section covers any occurrence of AI solutions being used by the supplier within the contractual arrangement. This can include AI within a system or application being provided or AI being used by the supplier, or their supply chain, while processing or managing information assets.

14.1 Your approach to AI development or its use as part of this contract must align with the NCSC guidelines for Secure AI System Development (https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf). Unless otherwise advised you are confirming compliance across areas of NCSC secure design, development, deployment, operation and maintenance.

14.2 The supplier, and their supply chain, must not use ERC data, information or telemetry data to train any AI model or system where that learned data set would/could be shared or used by parties other than the Council or agreed partners under a data sharing agreement. If the supplier does not meet this requirement they must inform the Council prior to any contractual arrangement.

14. Appendix 1 – Code of Connection Example

Protocol 1 Code Of Connection / Network Security Agreement

THIS AGREEMENT is made on the <Date> ("the Effective Date") between:

East Renfrewshire Council

having its principle office at Eastwood Park, Rouken Glen Road, Giffnock, G46 6UG

(hereinafter referred to as "ERC") and

<Third Party's name>

(hereinafter referred to as 'the Business Partner')

whose registered office is situated at: <location>

Whereas, ERC has determined that connection to the ERC ICT network, of one or more of the Business Partner's computer systems located at the Business Partner's premises at <insert name of relevant premises> (hereinafter referred to as the "communications link") is advantageous in order for agreed tasks of work to be completed in an effective manner;

and whereas ERC is prepared to grant the Business Partner the necessary access;

and whereas the Business Partner agrees to adhere to ERC's security policy and the conditions set out below regulating such access, in order for ERC to ensure that such access does not in any way compromise the interests of ERC, its information assets, computing and networking systems or its employees.

NOW THEREFORE IT IS AGREED BETWEEN THE PARTIES AS FOLLOWS:

1 Physical Link Connection

1.1 The communications link connection between the Business Partner (or a third party sub-contracted by the Business Partner to perform the task on their behalf) and the ERC ICT network is for use only for the agreed tasks of work contained in **Appendix A** to this Agreement. Should ERC consider that the communications link is being used in any other manner, ERC reserves the right to sever the communications link without notice and without prejudice to ERC's other rights and remedies arising from such misuse. ERC will not be liable for any loss or damage incurred through severance of the communications link.

1.2 No computer equipment other than that described in **Appendix B** to this Agreement may be used with the communications link. Should ERC determine that any other equipment has or had access to the communications link between ERC and the Business Partner, ERC reserves the right to sever the communications link without notice and without prejudice to ERC's other rights and remedies arising from such unauthorised access. ERC will not be liable for any loss or damage incurred through severance of the communications link.

2. Information Security

2.1 No information, data or software may be taken from ERC's computer systems other than that information, data or software specifically required to perform the task of work as described in **Appendix A**. The Business Partner shall apply appropriate protective measures to any information, data or software taken from ERC's computer systems and shall use all reasonable endeavours to ensure such information is not released to or accessed by any person other than employees of the Business Partner directly involved with the agreed task of work.

2.2 No information, data or software may be transmitted to ERC by the Business Partner or any other 3rd party source other than that information, data or software specifically required to perform the task of work as described in **Appendix A**.

2.3 The Business Partner shall comply and ensure that its employees will at all times adhere with the provisions and the obligations imposed by virtue of the Data Protection Legislation (Data Protection Act 2018 and the UK GDPR) in processing personal data and the Guidance issued by the Information Commissioner.

2.4 In processing personal data on behalf of ERC, the Business Partner shall comply with the said data protection principles at all times in accordance with the instructions of ERC as Data Controller and generally do nothing to compromise the Council's compliance with its obligations as data controller.

2.5 In the event that the actions or inactions of the Business Partner, whether deliberate or accidental, in respect of any unauthorised disclosure or other processing of personal data caused/undertaken by the Business Partner, result in a breach of the Data Protection Act 2018 then the Business Partner shall wholly indemnify ERC for any such breach.

3. Physical Security

3.1 Business Partners equipment which is electronically connected to the ERC ICT network must be located either:

- within the Business Partner's premises and not readily accessible by the general public. In addition, such equipment shall be located in areas within the premises of the Business Partner in such a manner as to limit physical access to the equipment to only those individuals requiring such access for the purposes of the agreed task of work.
- within Business Partner's staff households, where individuals are authorised to undertake home working and those staff have undertaken training to ensure access to ERC systems, networks and information remains secure and protected from unauthorised access.

4. Network & Communications Security

4.1 Items of IT equipment approved for use with the ERC ICT network may be networked together. However, no other network or communications link may be connected to any of the approved IT equipment while it is connected to the ERC ICT network, without the prior written consent of ERC Head of Digital & Community Safety, which consent shall not be unreasonably withheld.

5. Personnel Access

5.1 Use of the equipment connected to the ERC ICT network must be limited to only those personnel directly involved in the agreed task of work. An approved list of appropriate personnel who are qualified and trained to undertake work under this agreement must be agreed with ERC prior to the commencement of the task of work and must include, without limitation, name, location, business telephone number, normal working hours, and Computer User Identifier for each individual involved in the agreed task of work. The Business Partner shall notify ERC and request approval of any staff who are added to the approved list prior to any new person commencing the task of work.

5.2 Computer User Identifiers used by personnel of the Business Partner when accessing the ERC ICT network are to be unique. Each Computer User Identifier is to be used only by the individual to whom the Identifier has been allocated. Passwords associated with the user must not be shared, are to be changed on a regular basis (not exceeding 90 days), changed if it is suspected of being compromised and disabled when that user leaves the Business Partner's employment.

5.3 ERC reserves the right to carry out monitoring and random checks to ensure access to the ERC ICT network is only performed by those individuals on the approved list. In the event of non-approved personnel accessing the ERC ICT network, or any Computer User Identifier being used by any person other than the agreed individual, ERC reserves the right to sever the communications link without notice and without prejudice to

ERC's other rights and remedies arising from such unauthorised access. ERC will not be liable for any loss or damage incurred through severance of the communications link.

6. Scope of Communications

6.1 The ERC ICT network has been created and implemented in a manner which encourages the free exchange of information and services for all ERC personnel operating in ERC. No attempt shall be made by any personnel of the Business Partner to gain access to any information, equipment or services not directly concerned with the agreed task of work. Should any attempt be made to access information, equipment or services not directly concerned with the agreed task of work, ERC reserves the right to sever the communications link without notice and without prejudice to ERC's other rights and remedies arising from such attempt. ERC will not be liable for any loss or damage incurred through severance of the communications link

7. Checks and Reviews

7.1 The Business Partner shall provide to ERC full unrestricted access to check the location and integrity of any equipment located within Business Partners premises which has access to the ERC ICT network, at any time, and from time to time at the request of ERC. Such visits would be pre-arranged and agreed by both parties.

7.2 In the event of any significant reduction of security levels, whether temporary or permanent, for whatever reason the Business Partner shall alert the ERC Head of Digital & Community Safety and notify him/her of any additional security measures being put in place. ERC reserve the right to require that additional measures be implemented if those proposed do not match the required standard.

7.3 The Business Partner agrees to notify the ERC Head of Digital & Community Safety of any planned changes to the security specification of equipment with access to the ERC ICT Network, and obtain his/her consent prior to making the changes.

8. Personnel Behaviour

8.1 The Business Partner shall ensure that all Business Partner personnel with access to, and/or use of equipment connected to the ERC ICT network are made aware of, and operate in accordance with, the terms of this Agreement.

9. Notification of Security Incidents

9.1 The Business Partner shall provide to ERC the name of a designated employee, of appropriate seniority, who will act as the point of contact between the Business Partner and ERC in the event that an incident occurs which ERC considers to be in breach of this Agreement, irrespective of whether the event originates from the Business Partner or ERC.

9.2 The designated employee may be asked to supply to ERC any information or data (eg., system log files) from within the Business Partners organisation which is considered by ERC to be pertinent to the investigation of such an event.

9.3 In the event that the Business Partner becomes aware of a breach of this Agreement it shall immediately inform ERC and take all necessary actions to rectify this breach within 24 hours.

9.4 The Business Partner and ERC staff, as nominated by the ERC Head of Digital & Community Safety, shall investigate any security incident within one working day of any notification, or as soon as reasonably practicable thereafter. Use of the communication link may be suspended by ERC pending the outcome of such investigation.

9.5 ERC reserves the right to suspend or sever the communications link without notice and without prejudice to ERC's other rights and remedies arising from such incident. ERC will not be liable for any loss or damage incurred through severance of the communications link.

10. Indemnities

10.1 The Business Partner shall be responsible for and shall save, indemnify, defend and hold harmless ERC from and against all claims, losses, damages, costs (including legal costs) expenses and liabilities in respect of:

10.1.1 loss or damage to property of ERC whether owned, hired or leased relating to or in connection with the performance or non- performance of the agreement by the Business Partner or those for whom it is responsible in law; and

10.1.2 personal injury (including death or disease) to any person employed by ERC arising from or relating to or in connection with the performance or non- performance of the agreement by the Business Partner or those for whom it is responsible in law.

10.1.3 subject to the express provisions of this agreement, personal injury (including death or disease) to any third party or loss or damage to the property of any third party to the extent that any such loss, damage or injury is caused by the negligence or breach of duty (whether statutory or otherwise) of the Business Partner or those for whom it is responsible in law. For the purpose of this clause, 'third party' shall mean any party which is not ERC or the Business Partner

10.1.4 loss or damage to ERC's ICT network by viruses or trojan horses which are transmitted arising from or relating to or in connection with the performance or non-performance of this agreement by the Business Partner or those for whom it is responsible in law.

10.2 ERC shall be responsible for and shall save, indemnify, defend and hold harmless the Business Partner from and against all claims, losses, damages, costs (including legal costs) expenses and liabilities in respect of:

10.2.1 personal injury (including death or disease) to any person employed by the Business Partner arising from or relating to or in connection with the performance or non- performance of the agreement by ERC or those for whom it is responsible in law.

10.2.2 subject to the express provisions of this agreement, personal injury (including death or disease) or loss or damage to the property of any third party to the extent that any such loss, damage or injury is caused by the negligence or breach of duty (whether statutory or otherwise) of ERC or those for whom it is responsible in law. For the purpose of this clause, 'third party' shall mean any party which is not ERC or the Business Partner

11. Duration and Renewal

11.1 This Agreement shall subsist from the last date of signing hereof and shall automatically terminate thereafter unless renewed by mutual consent in writing. However, either party may terminate upon giving thirty days written notice to the other, or forthwith upon giving immediate written notice to that effect, where the other Party commits any breach of the terms of this Agreement.

12. Jurisdiction

12.1 This Agreement shall be governed by the Laws of Scotland and the Parties hereby prorogate the jurisdiction of the Scottish Courts.

13 Statement of Acceptance

13.1 The Business Partner has reviewed the foregoing standards and agree that all measures will be taken to ensure that access to the ERC ICT network and/or any equipment supplied by ERC will be exercised only in accordance with the terms of this agreement.

For and on behalf of ERC (to be signed by an accountable HoS engaging services of supplier)

Signed:_____ Name:_____

Position:_____ Dated:_____

For and on behalf of Business Partner (to be signed by an accountable senior manager)

Signed:_____ Name:_____

Position:_____ Dated:_____

Appendix A

Task to be performed as part of this agreement are:

- Any tasks associated with the ongoing support and Maintenance of the provided solution.
- Any other tasks as outlined in future agreed project plans and / or work packages.

Appendix B

Only equipment belonging to and subject to the security controls and processes of the service provider may be used to participate in a remote access connection to the East Renfrewshire Council internal network and / or any external 3rd party environment used for the purpose of hosting of ERC's Internet or Intranet platform.

Equipment to be used may be specifically identified as part of any future risk assessment.