Cyber & Information Management (Procurement)

Policy Statement

1. Introduction

1.1 Where information and personal data are processed on behalf of Gloucestershire County Council (GCC) by a contractor supplying goods and/or services, GCC retains responsibility for such information and personal data and is obliged, therefore, to ensure that it is processed efficiently and in accordance with the law. In view of this, it is important to ensure that the requirements set out in this policy are:

a. Included within the contractual obligations;
b. Observed and complied with; and
c. Regularly monitored by GCC commissioners and contract managers.

1.2 The level of information risk is not directly comparable to the contract value; therefore this policy is applicable in all circumstances where there is a contract in place between GCC and a contractor where the contractor will have access to personal data for which the council is the data controller. Including, but not limited to, circumstances where the contract includes GDPR related provisions and a schedule containing a detailed description of the subject matter, nature, duration and permitted categories of data processing. The standards identified in this policy will also apply where the loss or corruption of any data would cause significant impact to service delivery or reputational damage to the council.

1.2 GCC requires its contractors (including sub-contractors) to have in place relevant technical, physical and organisational measures (Protective Measures) to protect GCC data.

1.3 The council's preference is for its suppliers to achieve Cyber Essentials Certification as a minimum. This policy and the supporting documents set out the standards that GCC requires its contractors to comply with, taking into account the need to appropriately manage all relevant risks, as determined by GCC's Risk Assessment Tool available on Staffnet.

1.4 GCC requires all contractors to follow best practice guidance and have in place protective measures which comply with the following:

- National Cyber Security Centre (NCSC)'s 10 Steps To Cyber Security
- The Information Commissioner's Office (ICO) Practical guide to IT Security

1.5 Each tender exercise must assess which standard, or set of standards, is relevant to that particular procurement at the outset. Using this assessment, the Information Asset Owner (IAO) will determine the required accreditation level, in consultation with the Information Management Service (IMS).The contractor must then confirm adherence to the standard. As part of the ongoing contract management the most up to date accreditation will be sought by the relevant commissioner/contract manager.

January 2020

1.6 During the period from 1 January 2020 to 31 December 2020 all new GCC procurements

and subsequent contracts shall include, as a minimum requirement, provisions which require contractors, at their own cost, to conform to the relevant identified standard described, within 12 months of the contract commencement date.

January 2021

1.7 From 1 January 2021, all new GCC procurements and subsequent contracts shall include, as a minimum requirement, provisions which require contractors, at their own cost, to have in place and an up-to-date accreditation, which confirms they meet the relevant identified standard (set out in paragraph 2).

1.8 Where information risks are higher, as determined using the GCC's Risk Assessment Tool, contractors shall be required to have obtained certification (or demonstrate equivalency) in respect of at least one of the following standards, in addition to or in place of Cyber Essentials:

- Cyber Essentials Plus certification (or equivalent, see paragraphs 2.3 and 2.9)
- ISO27001 certification (or equivalent – see paragraphs 2.4 and 2.9)

1.9 As Cyber Essentials and ISO27001 do not cover all aspects of relevant technical security the standards will be supplemented by a requirements policy and/or questionnaire during the tender stage.

1.9 Where certification or accreditation is held by the contractor, demonstrating that it has obtained accreditation in respect of any of the standards set out in paragraph 2 (e.g. a Cyber Essentials Certificate), the relevant GCC commissioner/contract manager shall request a copy of such certification or accreditation from the contractor on each anniversary of the relevant contract. In cases where ISO27001 accreditation is in place, the relevant GCC commissioner/contract manager shall request a copy of the new certificate upon expiry of the accreditation.

1.10 Contractors shall be required to demonstrate to GCC that any of their staff, sub-contractors, or staff of sub-contractor who have access to GCC data, are aware of and comply with this policy.

1.11 Contractors shall be required to ensure that their sub-contractors with access to GCC data, including, but not limited to access, process, store or communicate information, or provide IT infrastructure components, shall have in place relevant Protective Measures, as determined using GCC's Risk Assessment Tool.

1.1.2 Non compliance with this policy, e.g. failure to provide relevant certification or complete equivalency requirements, will result in that contractor failing to obtain the contract.

1.1.3 Identified and assessed risks are to be signed off by the relevant Information Asset Owner (IAO), following discussions with IMS and/or ICT.

1.1.4 Any concerns about the level of risks being signed off by IAOs will be escalated by IMS to the SIRO for determination.

2. The Information and Cyber Security Standards

2.1 The invitation to tender documents for all contracts procured by GCC must identify which of the cyber security standards (set out in paragraphs 2.2-2.8), if any, are relevant to each contract and require the contractor therefore to confirm adherence to the relevant standard or demonstrate equivalency.

2.2 Cyber Essentials Certification

2.2.1 Cyber Essentials certification is awarded to organisations that can verify that they have implemented a set of controls which provide protection from the most prevalent forms of threat coming from the internet.

2.2.2 Contractors are required to undertake, via questionnaire, their own assessment of their implementation of the Cyber Essentials control themes, which is approved by the contractor's senior executive, such as the CEO. The questionnaire is then verified by an independent Certification Body to assess whether an appropriate standard has been achieved, and certification can be awarded. This offers a basic level of assurance and can be achieved at low cost.

2.2.3 Where this standard is met it is mandatory for contractors to demonstrate on an annual basis that they meet the technical requirements prescribed by Cyber Essentials for those contracts which are determined using GCC's Risk Assessment Tool as low risk.

2.2.4 Examples of where Cyber Essentials will be necessary include:

- Where personal information of citizens/service users/employees, such as name, date of birth, home addresses, phone numbers or other contact information is handled by a supplier.
- Where personal information of council employees or Elected Members, such as travel booking information, is handled by a contractor.
- Where the loss or corruption of data would cause significant impact to service delivery or reputational damage to the council.

2.3 Cyber Essentials Plus Certification

2.3.1 Cyber Essentials Plus certification is awarded to contractors that have implemented a set of controls which have been verified by an external assessor, therefore offering a higher level of assurance. Cyber Essentials Plus comprises remote and on site vulnerability testing to check whether the controls claimed actually defend against basic hacking and phishing attacks. It is therefore the more rigorous assessment and will be required when risk is assessed as higher.

2.3.2 Where this standard is met it is mandatory for suppliers to demonstrate annually (or more frequently if required) that they meet the technical requirements prescribed by Cyber Essentials Plus for those contracts determined using GCC's Risk Assessment Tool as medium risk.

2.3.3 Examples of where Cyber Essentials Plus will be necessary include:

- Where special category personal information of citizens/service users/employees, such as race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation, is handled by a supplier.
- Where financial information of GCC service users/employees, such as bank details, payments, payroll is handled by the supplier

2.4 ISO27001 Certification

2.4.1 ISO27001 certification is recognised globally as a benchmark for good information security practice, which enables contractors to achieve independent certification by an accredited certification body following the successful completion of an audit. Certification is likely to be required in respect of high risk procurements (as determined using GCC's Risk Assessment Tool available on Staffnet) where Cyber Essentials Plus will not provide sufficient assurance on its own.

2.4.2 ISO27001 certification demonstrates that a systematic approach to managing information has been adopted by the contractor in order to ensure that such information remains secure. The ISO27001 certification process includes an assessment of people, processes and IT systems by applying a risk management approach to help keep information assets secure and the maintenance of controls to protect against risk.

2.4.3 Examples of where ISO27001 certification will be required include:

- Provision of data centre services
- Large scale databases, e.g. Payroll and social care systems

2.5 PCI DSS (Payment Card Industry Data Security Standard)

2.5.1 The S151 Officer must approve all new card payments facilities and outlets offered by the Council.

2.5.2 PCI DSS is the worldwide Payment Card Industry Data Security Standard that was set up to help businesses process card payments securely and reduce card fraud. PCI DSS certification is awarded to contractors in order to certify that they have in place tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data.

2.5.3 This standard will apply to any contractor that accepts, transmits or stores any cardholder data on behalf of GCC.

2.5.4 The standard required will depend on the merchant level, as defined by Visa:

Merchant Level	Description
1	Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant — regardless of acceptance channel — processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year.

2.5.5 The council's Card Payment Policy can be found here: https://staffnet.gloucestershire.gov.uk/media/220968/card-payment-policy-v02.docx

2.5.6 More information is available at https://www.pcicomplianceguide.org/faq/

2.6 Data Security & Protection Toolkit.

2.6.1 The NHS requires, in relation to Adults and Public Health services, that the council's contractors have successfully completed a Data Security and Protection Toolkit or the council has assured itself separately that they reach a similar or higher data security standard (see paragraph 2.9 for equivalency).

2.7 Surveillance Cameras (CCTV)

2.7.1 The Surveillance Camera Code of Practice must be adopted in circumstances where a contractor provides surveillance camera services on behalf of the council under the following circumstances:

a) to observe public places
b) civil parking enforcement functions under the Traffic Management Act 2004
c) bus lane enforcement functions under the Transport Act 2000
d) licensing functions, where the use of surveillance camera systems is being considered as part of the conditions attached to a license or certificate.

2.8 W3C Web Content Accessibility Standards.

2.8.1 The council requires any public facing digital solutions to be perceivable, operable, understandable and robust for the people who need to use them, regardless of barriers in accordance with the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018. To achieve this GCC requires all digital solutions to be compliant with the W3C Web Content Accessibility Standards at level 2.1.

2.9 Equivalency

2.9.1 According to public procurement law, a contractor is not obliged to obtain Cyber Essentials or ISO27001 Certification. A contractor need only demonstrate, to the satisfaction of GCC, that they conform to GCC's Cyber Security Standards (i.e. equivalent security standards).

2.9.2 One method of demonstrating that a contractor conforms to GCC's required cyber security standards is for the contractor to obtain, at the contractor's own expense, verification by a technically competent and independent third party that such standards have been met. Alternatively, contractors may be requested to complete GCC's Security Standards Form, a copy of which is at [to be developed].

2.10 Council Standards

2.10.1 In addition to the standards set out in paragraphs 2.2-2.9 and the best practice identified in paragraph 1.4 the contractor shall also be required to observe and comply with the procedures and standards set out in GCC's "Information Security & Handling Standards for Contractors Policy" a copy of which is at [to be developed].

3. Exemptions

3.1 Under the detailed circumstances that follow at paragraphs 3.2-3.5 it is not necessary to apply the requirements specified under Cyber Essentials, however PCI DSS, ISO27001, DSP Toolkit, CCTV and W3C standards may still be applicable.

3.2 **The Government Digital Service**: responsible for the management of a number of schemes which already include comprehensive cyber security obligations. Accordingly, contractors operating under the following schemes are exempt from having to conform to the requirements of obtaining Cyber Essentials certification:

i) Digital Services Framework (DSF): DSF suppliers have been technically and commercially evaluated to provide a comprehensive choice for agile projects.
ii) Public Sector Network (PSN): PSN services are currently accredited against the network's security standards. In the future, PSN services will be assessed against Government's Network Security Principles.

3.3 **ID Assurance Framework:** Being able to provide your identity online easily, quickly and safely is recognised as a key enabler of internet use by the Government and its users.

Providers of public services such as national and local governments, major internet companies, online retailers, banks and others have to address business and security issues around identity proofing and username/password fallibility to mitigate the financial and administrative implications of identity fraud and compromise of personal data.

3.4 **Assisted Digital:** Assisted Digital is support for people who can't use online services independently.

3.5 **ISO27001:** Contractors holding ISO27001 certification, where the Cyber Essentials requirements, at either basic or Plus levels as appropriate, have been included in the scope, and verified as such, would be regarded as holding an equivalent standard to Cyber Essentials. Therefore, such contractors are exempt from the requirement to obtain Cyber Essentials certification, provided that the certification body (likely to be a consultancy) carrying out the ISO27001 verification is approved to issue a Cyber Essentials certificate by one of the accreditation bodies.

3.6 **Supplier Assurance Framework:** Procurements that follow the requirements outlined in the Supplier Assurance Framework and during this process have fully covered Cyber Essentials requirements will be exempt from the requirement to obtain Cyber Essentials certification. The Supplier Assurance Framework is at: https://www.gov.uk/government/publications/government-supplier-assurance-framework. Accordingly, such procurements are exempt from having to separately undertake Cyber Essentials.

3.7 **Low risk contracts:** If, in relation to any proposed contracts, the cyber security risk is assessed as very low, using GCC's Risk Assessment Tool, the contractor under such contract shall be exempt from the requirement to obtain the Cyber Security Standards certification. Contracts may be exempt where use of Cyber Essentials or other technical standard can be demonstrated to be either not relevant or clearly disproportionate, such as where a cyber security risk is assessed as very low. In such cases a decision audit trail must be recorded by the GCC commissioner/contract manager.

4. GCC Responsibilities

4.1 Information Asset Owners

- To determine level of information risk and relevant standard to apply.
- To own any residual information risks and determine appropriate action (e.g. accept, avoid, mitigate).
- To ensure appropriate contract monitoring is undertaken.

4.2 The Information Board

- To review and monitor strategic and significant information risks.

4.3 SIRO

- To determine risk appetite and make a determination on any escalated risks.
- To own strategic information risks and determine appropriate action (e.g. accept, avoid, mitigate).

4.4 DPO and Information Management Service (IMS)

- To develop and maintain support tools and guidance, including the information standards and a risk assessment tool.
- To support and advise IAOs in determining the level of information risk and relevant standard.
- To escalate significant risks to the SIRO, where appropriate controls are not considered to be in place or in progress.

- To develop plans for the mitigation of identified strategic and significant information risks.

4.5 ICT

- To assess technical equivalency requirements.
- To develop user friendly equivalency standards.

4.6 Commissioners / Contract Managers / Project Managers

- To ensure that IMS and ICT expertise is sought at the outset of commissioning, contract and project activities.
- To ensure that GCC requirements are made clear to potential contractors.
- To ensure that GCC standard contract clauses are used or to obtain equivalency assurance from legal service where alternative provisions are put in place.
- To obtain a copy of the certification/ accreditation on each anniversary of the contract.
- To ensure information risks are documented in local risk registers and any significant risks escalated to the Information Management Service.

4.7 Commercial Service

- To ensure that the requirements of this policy and accompanying standards are included in procedures and guidance.
- To ensure that GCC's contract management system includes appropriate performance measures to enable confirmation and monitoring of compliance with this policy.

4.8 Legal Service

- To ensure that contracts contain appropriate clauses to meet the requirements of this policy and data protection legislation.

5. Review and Revision

5.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

6. Document Control

Owner:	Jane Burns, Director, Strategy & Challenge (SIRO)
Author:	Jenny Grodzicka, Head of Information Management (DPO)
Last Reviewer:	
Create Date:	August 2019
Next review date:	June 2020
Approval:	Corporate Management Team (COMT), 12 September 2019
Version:	1-2

Version	Version date	Summary of Changes
1-1	10/01/2020	Included links to documentation on Staffnet
1-2	15/12/2020	Update to broken links