Primary Security Risk Assessment

A requirement of General Data Protection Regulation (GDPR) is for Warwickshire County Council (WCC) as Data Controller to perform a risk assessment on the systems/provider of the Data Processor regarding the Confidentiality, Integrity and Availability of data. See Article 32 of GDPR "Security of Processing" https://gdpr-info.eu/art-32-gdpr/.

Please note, there is no right or wrong way to answer these questions, it simply allows us to perform a risk assessment. Please answer the questions fully (even if it's just N/A) or it may delay the approval if we require further detail to provide assurance. The personal information (contact details) you provide are needed so we know which system we attribute the answers to and if we need to contact you for more information.

*Required

Email address *

Your email address

Please provide project/tender/contract reference *

or enter Not Known

Your answer

What is the system/service being tendered/provided *

Your answer

Please provide your company name, and your contact details. *

Your answer

Who are your contacts at WCC *

Your answer

Name and Details of your Data Protection Officer or nominated contact for DP *

Your answer

ICO Registration Number: *
or enter Not Registered

Your answer

Do you process personal data provided by WCC or collect/process on behalf of WCC *

- ○ Yes
- ○ No
- ○ N/A

Do you process special category personal data provided by WCC or collect/process on behalf of WCC *
Special category as defined by GDPR Article 9, or sensitive personal data as defined in DPA1998

- ☐ Yes
- ☐ No
- ☐ N/A

Names and addresses of any sub-contractors or organisation you shared the data with and specify the reason: *

Your answer

Location of personal data processed by you and any sub-contractors: *

Your answer

If you provide health/care services are you compliant with the NHS toolkit *

This was the IG Toolkit, now replaced by the Data Protection & Security toolkit in 2018. Enter YES if level 2 or 3 of the IGT, NO if level 1, N/A if not submitted/used or not relvant

- [ ] Yes
- [ ] No
- [ ] N/A

INFORMATION SECURITY CERTIFICATIONS

In regard to ISO 27001, please select each party that has current certification that processes data. If the systems that process data are NOT in the current certification Scope please select NO. *

	YES	NO	N/A
Have ISO27001 certification in our own right (The certificate is in our name)	○	○	○
DO NOT have ISO27001, but plan to.	○	○	○
Are using a hosting company that has ISO27001 Certification	○	○	○

Cyber Essentials Plus. CE+ was designed for suppliers to Central Government as a baseline of technical controls. Please mark each statement for correctness. (i.e. do not plan is YES if you do not plan to obtain it) *

	Yes	No	N/A
We already have CE+	○	○	○
We Plan to obtain CE+	○	○	○
We do NOT plan to obtain CE+	○	○	○

CONFIDENTIALITY

These questions pertain to the controls in place to ensure the data, confidentiality. These include Account Management, Security of the Computers the Data is Processed on and how the Data is transferred.

Thinking about Account Management, what controls do you have in place for your staff with administrative access to our data. *

Controls of interest include who has access to privileged accounts (Administration Accounts), How the permissions are set on the data (Least Privilege) and how you deal with your Starters and Leavers. We've made assumptions like password complexity.

Your answer

Thinking about encryption, please answer the following statements? *

	Yes	No	N/A
We use HTTPS	○	○	○
We use HTTPS and change the server configuration to make it stronger by removing old items.	○	○	○
We use database encryption for when the data is 'stored at rest'	○	○	○
We use file system encryption on our servers to ensure the data is encrypted at rest	○	○	○
We use encryption on our laptops to protect the data if the device is lost	○	○	○
We use encryption on our mobile devices that have the potential to access WCC data incase they are lost.	○	○	○

Do you use Pseudonymisation for test and training systems? *

Pseudonymisation is a process of making personal data unreadable but keeping a primary key so it can be worked back to a data subject. It is primarily used for "Secondary Use" such as statistics. It should really also be used for test and training systems so although there is text in a field - its not based on a natural person or data subject.

- ○ Yes
- ○ No
- ○ N/A

Thinking about systems security that process WCC Data please answer *

	Yes	No	N/A
Are your systems protected by a Network Firewall and is it actively managed?	○	○	○
Are your systems protected by a Local Firewall and are these actively managed/changed from default configuration?	○	○	○
Do all your systems have Anti Malware software and managed to ensure they are kept up to date?	○	○	○
Is your computer operating system managed so that the default security settings are changed to suit your environment	○	○	○
Do you have an active programme in place to ensure that software patches are applied ASAP?	○	○	○

What other controls do you have in place that prevent unauthorised access to WCC Data by either your own employees or attackers? *

A starter for 10 may include Audits, Active Monitoring, Segregation of Duties, Contractual etc.

Your answer

INTEGRITY

In terms of Integrity when it comes to security of WCC Data, we mean that it cannot be modified, deleted, stolen/removed in an undetectable manner. We don't expect the detection to be immediate but we are interested in how you would detect it. I can also tie in heavily when it comes to detecting a breach, so you can notify us immediately.

Do you have any of the following controls in place? *

	Yes	No	N/A
Does your system processing our data hold an audit item of any deletion or modification of data?	○	○	○
Are exceptions actively looked for?	○	○	○
Are exceptions manually looked for?	○	○	○
Do you perform your own formal risk analysis on the integrity of data you process and what controls you could select?	○	○	○

Are there any other controls for enforcing integrity when processing WCC Data, these may include RAID hard drives in servers, hashing data in databases, anything that can detect a change in data. *

Your answer

AVAILABILITY & RESILIENCE

Availability and Resilience are closely related, and where outages occur GDPR is concerned about not only about there are controls to

Do you have any of the following controls in place for systems processing WCC data? *

	Yes	No	Not Sure	N/A
Load Balanced systems	○	○	○	○
Clustered Systems	○	○	○	○
Uninterruptible Power Supplies	○	○	○	○
Multiple Data Centres	○	○	○	○
Multiple Network Links	○	○	○	○

Are there any other significant controls for availability that you want to let us know about? *

Your answer

NOTIFICATION & REPORTING

With regard to GDPR the reporting of a breach to the ICO is the responsibility of the Data Owner within 72 hours. The Data Processor has to immediately report any breach as per WCC's Standard Terms and Conditions.

In the event of a data breach of WCC data, do you/would you... *

	Yes	No	Partial	N/A
Have a process to isolate the relevant log files to assist with an investigation?	○	○	○	○
Have a process to isolate the affected systems to investigate the root cause or provide evidence to law enforcement?	○	○	○	○
Have a contact at WCC whom you immediately report the breach or suspected breach to?	○	○	○	○
Have a process for dealing with our WCC contact?	○	○	○	○

Send me a copy of my responses.

Page 1 of 1

SUBMIT

Never submit passwords through Google Forms.