Custodia Continuity

Cyber Security Self Questionnaire

HELLO!

Thank you for downloading this document - we hope it will help you decide how at risk you may be to a data breach or cyber-attack.

The twenty questions below are a simple and brief assessment framework that will give you a good idea of where to start in when figuring out your business's risk.

If you find you are answering **yes** to all the questions, then brilliant - you are likely to be heading in the right direction.

If you are answering **no** or **don't know** to most of the questions, then don't worry; we are here to help.

Give us a call and we can advise you on your next steps and if you think you need us we can start a relationship together to help put any concerns you may have to bed and to make your business competent, compliant, resilient and ready for business in the 21st century.

If you need any support, if you have any questions about this document or you would just like to chat further about your needs, give us a call, drop us an email or contact us through our website, and one of our amazing team will be on hand to help.

Custodia Continuity
01629 369250

help@custodiauk.com

www.custodiauk.com

If you would like to write to us, then it's:

Custodia Continuity
The Old Blacksmiths
The Dale
Wirksworth
Derbyshire DE4 4EJ

We are here to help - we don't do hard-selling, we don't apply pressure or create fear.
We love answering questions and we love to meet new people and help solve problems.

We look forward to hearing from you.

Custodia Continuity

Cyber Security Self Questionnaire

Chris and Jae – Directors; Custodia Continuity

20 QUESTIONS

IT and HARDWARE

1. Do you virus-scan all of your computers (desktops and laptops) at least once a week?

2. Are all your business computers' hard disks encrypted?

3. Do all your employees have their own personal log-ins to work computers?

4. Do you tell employees NOT to use their personal computers for work?

5. Do you supply employees with portable IT equipment owned and controlled by the business?

6. Do you require employees to change their passwords regularly? Do you change passwords to any cloud services regularly?

7. Do you train your staff in cyber-security awareness?

NETWORK

1. Do you have a firewall on your network(s)?

2. Do you log access and traffic on your network(s)?

3. Do you use a guest WIFI network for visitors?

4. Do you change WIFI passwords regularly?

MOBILE

1. Do you supply work mobile devices?

2. Do you prevent employees accessing work materials on their personal mobile phones and devices?

BACKUP

1. Do you backup all your essential data at least once a day to a location outside your office? How often do you test your backups?

2. Do you have a clear recovery plan, should you have a data breach or ransomware attack?

DATA PROTECTION

1. Do you have up-to-date policies (8 changes to GDPR since May 2018) in place covering IT, Data Retention, GDPR (DPA)2018?

2. Are your staff trained in data protection awareness? For instance, what should they do about a subject access request?

3. Are your website(s) cookie-consent compliant?

4. Are you aware of where all your data is stored and who has access to it?

5. Could you delete, upon request, a subject's personal data?