

What is Access Control?



The general principle behind the access control is that there should be policies and procedures in place that only allow users to access the business information that is required to deliver their job role.

Protecting user accounts and helping prevent misuse of administration accounts is essential for any cyber secure system or network.

User accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals and managed continuously to ensure that you are not leaving the business exposed for a hacker to take advantage of.

When privileged accounts are compromised their level of access can be exploited, maximising the damage the breach could cause the business.

To protect against misuse of special access privileges, the principle of a need to know basis should be applied to user accounts by limiting the privileges granted and restricting access.

Is your business guilty of any of the below statements?

Lack of unique username and strong password policy?

Setting users up with privileges that they don't need?

Lack of user privilege management system?

Why Choose Axiom?

- We are a trusted provider of end-to-end cyber security solutions
- We tailor solutions to fit your needs
- We provide experienced consultants at all stages of any engagement.
- Our team understand the current cyber risk vulnerabilities and provide business solutions to mitigate these risks

Access Control is one of the five key controls that form the focus of Cyber Essentials

Contact Us Now

Axiom Cyber Intelligence
0333 355 8553
info@axiomci.co.uk
www.axiomci.co.uk