Cybersecurity consultancy: Information Security policy writing

ramsac
the secure choice

Why do organisations need an Information Security policy?

Humans are usually the weakest point of an organisation's defence against security breaches. Hence employees require a rule book that gives them guidance to better protect the organisation's data wherever it may be stored. An Information Security policy approved by the board demonstrates a positive stance on cybersecurity to both employees and customers.

What is an Information Security policy?

An Information Security policy details the overall approach to safeguarding an organisation's data. It contains procedures, processes, policies and security Dos and Don'ts that all employees should follow to achieve confidentiality, integrity and availability of an organisation's data and systems. Furthermore, having a security policy in place and implementing the content of this policy is strongly recommended by the Information Commissioner's Office (ICO). Other security best practice standards such as Cyber Essentials, ISO27001 and other globally recognised standards require every organisation to have an Information Security policy in place.

How can ramsac help?

Writing a security policy can be quite time consuming and daunting. Many organisations end up writing a generic policy that does not capture their approach to security and doesn't provide proper security guidance for employees.

ramsac can help you do the heavy lifting by writing a jargon free security policy that is easily readable and understandable by your employees and relevant third parties and that truly reflects your organisation's approach to security.

ramsac
the secure choice

Information Security policy writing: What's involved

Scoping call - The scoping call allows us to understand your business, the scope of the policy and what areas would provide value to the policy.

Information gathering - During this step we speak to stakeholders and gather information on your current security processes and procedures, available policies and any other relevant Dos and Don'ts that would help improve your security.

Write up - During this phase using all the information gathered about your current security posture, we write a policy that truly reflects your organisations security capabilities and rules employees should follow to protect your corporate data and data processing systems.

Review meeting - After writing your security policy, we review this policy with you to explain what has been covered, respond to any queries you might have and highlight any necessary updates that may need to be effected.

Follow up - After the review meeting, we will make final updates to the policy after which you are ready to share your security policy with your employees and all other relevant third parties.

Cybersecurity consultancy from ramsac

Utilising over 30 years experience supporting customers with their IT issues, our cybersecurity consultants can help protect your organisation against cybercrime.
ramsac's cybersecurity consultancy includes:

- Information security policy review
- Information security policy writing
- Breach Response Plan
- Cyber audit
- ISO 27001 consultancy
- General compliance queries

Find out more

Writing a security policy can be quite time consuming and daunting. Contact us for more information on how we can help your organisation to create a comprehensive security policy.

Tel: **01483 412 040** email **info@ramsac.com**