

Cyber security policy template

This template is designed to help small businesses create a cyber security policy tailored to their operations. It provides prompts to help businesses set out the measures, responsibilities and procedures they use to protect their systems, data and people from cyber threats.

This template provides general guidance only and should not be considered financial, legal, cyber security, IT or professional advice. You should adapt it to reflect your business's circumstances, requirements and cyber risks, and seek independent professional advice where appropriate. The controls included within your policy should be proportionate to the nature, size and cyber risks of your business. You remain responsible for deciding whether the completed policy is suitable for your business and compliant with any applicable legal or regulatory requirements. Completion of this template does not guarantee protection against cyber incidents and does not in itself affect the availability, terms or operation of any insurance policy. Markel Direct will not review, verify or approve policies completed using this template and does not accept responsibility for decisions made based on its contents.

This template should be reviewed regularly to ensure it remains appropriate for your business, technology and cyber security risks.



MARKEL

Company information

Business name: _____
Policy owner: _____
Date implemented: _____
Review date: _____
Policy version: _____

Policy purpose

Explain why your business needs this policy and identify the information, systems, devices and people it is intended to protect.

Example considerations:

- Customer information
- Employee information
- Financial data
- Business systems
- Company devices

Your policy statement:

Scope

Who does this policy apply to?

- ☐ Employees
- ☐ Directors
- ☐ Contractors
- ☐ Temporary workers
- ☐ Volunteers
- ☐ Suppliers with access to your systems or data
- ☐ Other: _____

List any business systems, devices or networks covered by this policy:

Roles and responsibilities

Individual(s) responsible for cyber security: _____

Their responsibilities:

Responsibilities of employees and other policy users:

Password requirements

Set out the password requirements that people covered by this policy are expected to follow.

Requirement	Your policy
Minimum password length	
Approved password manager	
Multi-factor authentication required?	Yes / No
Password review or change requirements	
Additional requirements:	

Email security

Outline how email should be used safely within your organisation.

Questions to consider:

- How should suspicious emails be reported?
- What should employees do before opening attachments?
- When should links be treated as suspicious?
- Who should employees contact if they believe they have received a phishing email?

Your requirements:

Remote working security

Select and add the security requirements that apply when working remotely or away from your usual workplace.

☐ Use company-approved devices

☐ Use secure Wi-Fi

☐ Use a VPN

☐ Lock devices when unattended

☐ Store equipment securely

Additional requirements:

Data protection

Describe how personal and confidential information should be handled.

Consider:

• Access controls

• Data storage

• Data sharing

• Data retention

• Applicable data protection requirements, including the UK GDPR

Your procedure:

Approved software and systems

List the approved software, platforms and security tools used by your business, including the provider or system name where known.	
Security measure	Provider/system
Antivirus software	
Firewall	
Backup solution	
Multi-factor authentication solution	
Software updates and security patches	
Device encryption	
Other	

Social media and internet use

Describe acceptable use of: • Company social media accounts • Personal social media during work • Company internet access Your requirements:
--

Reporting a cyber security incident

Anyone covered by this policy should report suspected or confirmed cyber security incidents to:

Name: _____

Role: _____

Telephone: _____

Email: _____

Examples of incidents to report:

- ☐ Phishing emails
- ☐ Lost or stolen devices
- ☐ Unauthorised access
- ☐ Malware or ransomware
- ☐ Data breaches
- ☐ Other suspicious activity

Cyber incident response

Document your organisation's response process.

Stage	Responsible person	Actions or procedure
Identify the issue		
Contain the threat		
Investigate the incident		
Notify affected parties		
Restore systems		
Review lessons learned		

Additional requirements:

Employee training

How often will cyber security training be provided?

- ☐ On induction
- ☐ Annually
- ☐ Every six months
- ☐ Following an incident
- ☐ Other: _____

Policy breaches

Describe how suspected or confirmed breaches of this policy will be investigated and managed.

Policy review

This policy will be reviewed:

- ☐ Annually
- ☐ After a cyber security incident
- ☐ Following major business changes
- ☐ Other: _____

Policy approval

Approved by: _____

Position: _____

Signature: _____

Date: _____



Discover help and guidance for small businesses and self-employed professionals in our [knowledge centre](#) and read more about our [small business insurance solutions](#).

Markel Direct
82 King Street, Manchester, M2 4WQ
T: 0800 640 6600 W: www.markeluk.com

