

Information Security Checklist



In an increasingly digital world, information security is of paramount importance for SMEs in England and Wales. Boardify's Information Security Checklist offers a comprehensive guide for organisations to protect their sensitive data and systems from potential threats. By making this checklist accessible, Boardify supports SMEs in strengthening their cybersecurity posture, minimising the risk of data breaches, and maintaining the trust of their customers and partners.

Policy Development

- Develop an information security policy and framework
- Ensure compliance with applicable laws, regulations, and industry standards
- Regularly review and update policies to reflect changes in the threat landscape and best practices

Risk Assessment

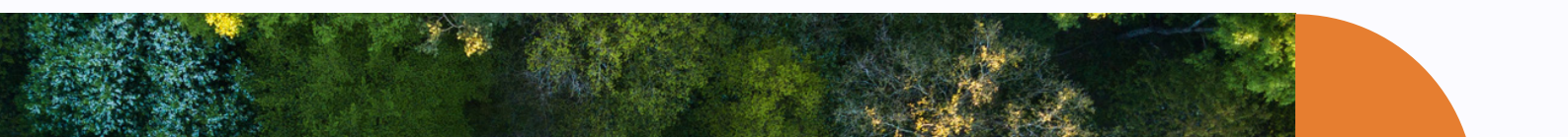
- Conduct regular information security risk assessments
- Identify vulnerabilities and potential threats
- Prioritise risks and develop mitigation strategies

Technical Controls

- Implement appropriate technical controls (e.g., firewalls, encryption, access controls)
- Regularly update software and systems to address security vulnerabilities
- Establish processes for secure data disposal

Physical Security

- Secure physical access to facilities and IT assets
- Implement measures to prevent unauthorised access, theft, or damage to equipment



Incident Response and Business Continuity

- Develop an incident response plan to address security breaches and incidents
- Establish a business continuity plan to ensure the availability of critical systems and data
- Regularly test and update plans

Training and Awareness

- Provide regular information security training for employees
- Communicate the importance of information security and employee responsibilities

