Cybersecurity Checklist

Cybersecurity is a critical concern for SMEs in England and Wales, as cyber threats continue to evolve and increase in sophistication. Boardify's Cybersecurity Checklist offers a comprehensive guide for organisations to develop and implement robust cybersecurity programs. By providing this resource, Boardify supports SMEs in enhancing their cyber defences, minimising the risk of security breaches, and protecting their valuable digital assets.

Policy Development

● □ Develop a comprehensive cybersecurity 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 cybersecurity 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

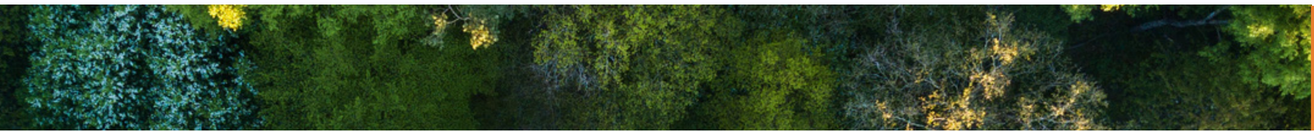
● □ Establish processes for secure data disposal

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 cybersecurity training for employees

● □ Communicate the importance of cybersecurity and employee responsibilities

● □ Conduct phishing simulations and other awareness activities to reinforce best practices

Monitoring and Detection

● □ Implement systems for continuous monitoring and detection of potential cyber threats

● □ Develop processes for rapid assessment and response to security incidents

Third-Party Risk Management

● □ Assess the cybersecurity risks associated with third parties, such as vendors and partners

● □ Implement contractual provisions and monitoring mechanisms to ensure third-party compliance with cybersecurity policies

Regulatory Compliance

● □ Ensure compliance with applicable data protection and privacy laws

● □ Address any regulatory inquiries or investigations related to cybersecurity

Continuous Improvement

● □ Assess the effectiveness of cybersecurity programs

● □ Identify areas for improvement and implement changes

● □ Foster a culture of vigilance, transparency, and accountability in cybersecurity