Australian Institute of Company Directors

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

Cyber Security Governance Principles Checklist for SME and NFP Directors

Principle 1: Set clear roles and responsibilities

□ Document, where possible, who has responsibility for cyber security

□ Appoint a cyber 'champion' to promote cyber resilience and respond to questions

□ Consider whether a director, or group of directors, should have a more active role in cyber security oversight

□ Identify our key digital providers and understand their cyber controls

Principle 2: Develop, implement and evolve a comprehensive cyber strategy

□ Proactively identify low-cost opportunities to enhance cyber capability

□ Assess whether utilising reputable external providers will enhance cyber resilience compared with managing in-house

□ Identify key operational and customer data, who has access to the data and how it is protected

□ Limit access to key systems and data and regularly review access controls

□ Regularly repeat cyber security training and awareness among all employees

□ Promote strong email hygiene (e.g. avoid suspicious email addresses and requests for login or bank details)

Principle 3: Embed cyber security in existing risk management practices

□ Patch and update applications and anti-virus software

□ User application hardening – limit interaction between internet applications and business systems

□ Limit or restrict access to social media and external email accounts

□ Restrict use of USBs or external hard drives

□ Restrict operating system and software administrative privileges

□ Implement multi-factor authentication

□ Maintain and regularly test offline backups of critical data

□ Ensure that departing employees and volunteers no longer have access to systems and passwords, or physical access to sites or sensitive data

Principle 4: Promote a culture of cyber resilience

- □ Mandatory training and phishing testing for all employees, and volunteers where appropriate
- □ Regular communications to employees on promoting strong cyber practices, including email hygiene. The communications could be electronic (e.g. email reminders) or physical (e.g. signage in the workplace)
- □ Incentivise strong cyber practices, for example small rewards for performance on phishing exercises
- □ Pick a staff member to be a 'cyber security leader' to promote strong cyber practices and respond to questions from other staff
- □ Subscribe to ASD alerts to stay across emerging cyber threats

Principle 5: Plan for a significant cyber security incident

- □ Prepare a Response Plan, utilising online templates if appropriate
- □ If practical, conduct a simulation exercise or test various scenarios against the incident response plan
- □ Ensure physical back-ups of key data and systems are regularly updated, tested and securely stored
- □ Maintain offline lists of who may assist in the event of a significant cyber security incident and which key stakeholders to communicate with

Comprehensive guidance for directors is contained in the *Cyber Security Governance Principles* from the AICD and the CSCRC

ACKNOWLEDGEMENT OF COUNTRY

The Australian Institute of Company Directors acknowledges the First Nations people across this Country. We acknowledge the Traditional Custodians of the Lands on which our organisation is located and where we conduct our business. We pay our respects to the Elders, past and present, and recognise those who continue to promote and protect First Nations cultures. The Australian Institute of Company Directors is committed to honouring First Nations peoples' unique cultural and spiritual relationships to the Skies, Lands, Waters, and Seas, and their rich contribution to society. We acknowledge the past and stand together for our future.

ABOUT CSCRC

The CSCRC develops cyber security capability and capacity to help keep Australia safe. We do this by developing innovative, real-world research and cultivating outstanding talent to solve pressing cyber security challenges for the nation.

ABOUT AICD

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and not-for-profit sectors.

DISCLAIMER

The material in this publication does not constitute legal, accounting or other professional advice. While reasonable care has been taken in its preparation, the AICD and CSCRC do not make any express or implied representations or warranties as to the completeness, reliability or accuracy of the material in this publication. This publication should not be used or relied upon as a substitute for professional advice or as a basis for formulating business decisions. To the extent permitted by law, the AICD and CSCRC exclude all liability for any loss or damage arising out of the use of the material in the publication. Any links to third-party websites are provided for convenience only and do not represent endorsement, sponsorship or approval of those third parties, any products and services offered by third parties, or as to the accuracy or currency of the information included in third-party websites. The opinions of those quoted do not necessarily represent the view of the AICD and CSCRC. All details were accurate at the time of printing. The AICD and CSCRC reserve the right to make changes without notice, where necessary.

COPYRIGHT

For more information about Cyber Security Governance Principles | Version 2 November 2024, please contact:

E: policy@aicd.com.au

JOIN OUR SOCIAL COMMUNITY

aicd.com.au

CCT1571_24