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