MinterEllison Cyber Security Best Practice Guide

In the evolving landscape of cyber security, not-for-profit organisations are increasingly becoming targets for cybercriminals, with the Australian Cyber Security Centre reporting that the average cost of cybercrime for small to medium-sized businesses ranges from $46,000 to $100,000.

Given often limited resources and a high reliance on community trust, it is crucial for these entities to adopt a robust cyber security posture. MinterEllison has prepared this checklist to provide a concise guide on best practices for cyber security within the not-for-profit sector. The checklist covers essential actions that can significantly bolster your organisation's defences against cyber threats, from cultivating a culture of awareness and vigilance to implementing technical safeguards like Multifactor Authentication (MFA) and DMARC (Domain-based Message Authentication, Reporting & Conformance).

By following the actions in this checklist, your organisation can not only protect its valuable data and resources but also maintain the integrity and trust that is the cornerstone of your mission.

For assistance in implementing any of these items either internally or through your Managed Service Provider (MSP), please contact MinterEllison to discuss how we can help to secure your IT environment.

Shannon Sedgwick
Partner
Technology Consulting

T +61 2 9921 4277 **| M** +61 481 102 121
shannon.sedgwick@minterellison.com

Keith Rovers
Partner
Social Impact Practice

T +61 2 9921 4681 **M** +61 411 275 823
keith.rovers@minterellison.com

Cyber Security Essential Actions for Organisations

This checklist outlines the Top 10 actions organisations should complete to enhance their cyber security posture. Refer back to this guide when discussing security controls with your MSP/IT Provider.

Top 10 Cyber Security Actions	Date Completed
Implement multi-factor authentication where possible to add a critical security layer, especially for high-risk actions like authorising significant payments or remote access to your IT environment.	
Implement DMARC and spam filters, while keeping email systems regularly updated for optimal email hygiene.	
Ensure your backup schedule aligns with your operational needs to avoid disruption in case of data loss.	
Limit administrative access privileges to essential personnel and conduct regular audits of account privileges and roles.	
Understand your service level agreements with your MSP comprehensively, especially regarding incident response and support services. This also applies to your cyber insurance policy where it is important to understand inclusions, exclusions, and how incident response decisions can affect your coverage.	
Develop a detailed incident response plan that includes step-by-step actions, key contacts, and notification protocols for regulatory bodies.	
Deliver targeted cyber security education regularly, focusing on the most common threats to your organisation, like phishing and malware.	
Implement a minimum of Essential 8 maturity level 1 by applying its controls throughout your systems, including personal devices used for work.	
Establish regular and transparent communication with your MSP to discuss and understand what security standards apply to your environment and how they ensure compliance is maintained consistently. (e.g. Essential 8, ISO 27001, NIST CSF)	
Utilise free cyber security resources and guidance from government organisations such as the Australian Cyber Security Centre and the Office of the Australian Information Commission, which can be found at: Small business cyber security guide | Cyber.gov.au; Privacy for not-for-profits, including charities | OAIC	

MinterEllison Consulting.