CYBER PRECEDENT

Strengthening the
legal profession's
defence against
online threats

THE AUSTRALIAN SIGNALS DIRECTORATE'S AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUAL

In 2016 the Australian Signals Directorate released a comprehensive three-part Australian Government Information Security Manual (the Manual) as part of its efforts to reduce the impact of cyber criminals on Australian Government business. The Manual provides guidance to Australian Government Agencies seeking to develop and implement informed risk-based information security policies and procedures.

Legal practitioners who engage and share information with Government Agencies may have contractual requirements to ensure their policies are consistent with the Manual. The Manual is also a useful starting point for practitioners to understand the risks arising from the activities of cyber criminals and to develop practical strategies to avoid, or minimise, those risks.

ABOUT THE MANUAL

The first part of the Manual is the Executive Companion targeted towards senior executives of government agencies. It provides a broad overview of the threat environment, the tools and techniques to counter cyber threats, and the users who are targeted by malicious actors, including cyber criminals. It provides five key questions management needs to consider when countering the cyber threat:

1. What would a serious cyber security incident cost our organisation?
2. Who would benefit from having access to our information?
3. What makes us secure against threats?
4. Is the behaviour of my staff enabling a strong security culture?
5. Are we ready to respond to a cyber security incident?

The second part titled the Principles Manual is aimed at Security Executives, Chief Information Security Officers, Chief Information Officers and senior decision makers across government. It provides a deeper understanding of the cyber threat environment and describes the expectations of Australian governments agencies in taking a risk management approach to information security. It emphasises that the agency is responsible for any cyber security incident, and the need to balance the operation and economic costs of information security measures with the need to protect information and systems. Where acceptable risks have been identified, they need to go through a formal approval process. Other principles in the Principles Manual relevant to the legal profession engaging with Government Agencies cover cloud computing, cyber security incidents, physical security, communications systems and devices, media security, software security, product security, email security, network security and working off-site.

The third part of the Manual is the Control Manual, updated in 2017. It is aimed at IT Security Advisers, Managers and security practitioners across government. It applies to any organisation that has entered into a Deed of Agreement with the Government to have access to sensitive or classified information. It provides a set of detailed controls which, when implemented, will help organisations and agencies adhere to the higher-level Principles document. It identifies risks faced by agencies, whether non-compliance presents an acceptable level of risk and the consequences of non-compliance with advised security controls.