CYBER
SAFE ORGANISATION

SAFEGUARDING ORGANISATIONS WITH
COMPREHENSIVE CYBERSECURITY

With cyber-attacks increasing in frequency and complexity we have seen a heightened level of malicious cyber activity in recent years.

Cybercrime can cause financial and reputational damage, disrupt business and essential services, and result in permanent damage to an organisation. In the 2023 financial year 94 thousand cybercrime reports were made in Australia. Ransomware remains the most destructive cybercrime threat to Australian entities – around 10 per cent of all cyber security incidents. Ransomware groups are constantly evolving to maximise their impact by targeting the reputation of Australian organisations.

Australian organisations, and even individuals, are also being targeted by malicious cyber actors. Malicious actors persistently scanned for any network with unpatched systems, sometimes seeking to use these as entry points for higher value targets. Applying patches to applications and operating systems is critical to ensuring the security of systems.

ABOUT **US**

KIRRA Services delivers experienced and comprehensive cybersecurity solutions to support your organisation to mitigate cyber security incidents. Our consultants bring over 20 years experience securing Australian government agencies. They have worked to develop and refine methods for detecting and mitigating targeted cyber intrusions of Australian government IT systems and networks.

We are also a Defence Industry Security Program 2 (DISP) member with the ability to sponsor security clearances and support organisations to meet DISP cyber requirements.

ASSESS: A comprehensive assessment of the current cybersecurity maturity is undertaken to evaluate the current security practices and identify gaps or vulnerabilities within systems.

MITIGATE: Advanced threat detection including intrusion detection, firewall protection, antivirus and malware. We secure network infrastructure by implementing strong access controls, secure configurations, and regular security audits. Our Incident Response includes real time monitoring, alerts, patching and data protection to address threats and vulnerabilities.

PENETRATION: Penetration testing including controlled security assessments to test and detect vulnerabilities and simulate real-word scenarios to ensure the best possible defence against a cyber threat.

MONITOR: Ongoing monitoring and evaluations to ensure your cyber solution remains at the front of the game and responsive to emerging and evolving cybers threats and compliance requirements.

SUPPORT: Ongoing technical support, including service implementation, configuration, and troubleshooting. Training resources and user documentation and certified cyber training courses and vendor certifications from beginner, intermediate to advanced.

www.kirraservices.com.au/cyber