Navigating the evolving cybersecurity landscape?

We are here to guide and advise you.

securestate
INFORMATION SECURITY & TECHNOLOGY

Who

Secure State provides advice to help improve and safeguard Australian businesses from cybersecurity threats and incidents. We have helped all different types of businesses, small and large, to better position themselves with policy, infrastructure and IT support.

What

Our offering of Cyber Core Essentials provides expert cybersecurity leadership on a flexible basis, enabling organisations to strengthen their security posture without the full-time cost.

Why

Know that you have experts monitoring, reviewing, strategising and communicating the latest in IT and cyber security relevant to your field in one manageable monthly payment.

Contact us.

08 8151 3096

info@securestate.com.au

Daily

- 24/7 monitoring and alerting of potential cyber risks
  - Subscribed Security Operations Centre (SOC) combines the benefit of automation and a team of always-on security professionals
  - Automated remediation steps and recommendations will ensure you're kept safe and updated at all times
- Access to cybersecurity online training
  - Keep up to date on latest threats and scams by ensuring your staff is trained

Monthly

- vCISO meetings
  - Develop strategies to mitigate risks
    - develop a tailored security strategy that aligns with the unique risks, objectives, and compliance requirements ensuring a customised approach to cyber threats.
  - Strategies to harden any cybersecurity gaps within organisation
    - evaluate potential threats and devise strategies to mitigate them before they can disrupt your operations
- Phishing simulations and reporting
  - Increase awareness and preparedness of staff about the ever changing phishing tactics used by cybercriminals
  - Develop a culture of quickly recognising and reporting on suspicious emails

Pricing starting from $995*

Value at $2,195

(*per month, up to 25 staff)

Quarterly

- Review of DISP / CMMC / Cybersecurity Framework Policies and procedures
  - Ensure you comply with whichever cybersecurity framework you align with
  - Have clear and concise updates on your cybersecurity framework and ensure you comply with latest regulations

Annually

- IRP review
  - Ensure you're prepared and have all strategies ready in the event of a cybersecurity breach
  - Mitigate potential damage following a cybersecurity breach
  - Improve communications, internally and externally
  - Be confident that processes are in place and your staff know what to do in the event of a breach