ACSC

ACSC Guidelines

Australian Cyber Security Centre Compliance

Aligned 2024

QuantSec Pty Ltd

Australian Cybersecurity Solutions Provider

Website: www.quantsec.com.au | Email: compliance@quantsec.com.au

Overview

The Australian Cyber Security Centre (ACSC) is the Australian Government's lead agency for cyber security. The ACSC provides comprehensive cybersecurity guidance to help organizations protect themselves against cyber threats and implement effective security controls. QuantSec maintains full alignment with ACSC guidelines, ensuring our security practices meet the national cybersecurity standards set by Australia's premier cyber security authority.

Our alignment with ACSC guidelines demonstrates our commitment to following Australia's national cybersecurity best practices and implementing security measures that protect against current and emerging cyber threats. This alignment ensures that our security approach is consistent with the strategies and frameworks endorsed by the Australian Government for defending critical systems and sensitive information.

Key Compliance Areas

Our alignment with ACSC guidelines encompasses the following critical security domains:

- **National cybersecurity best practices:** Implementation of security controls and processes recommended by ACSC to protect against sophisticated cyber threats targeting Australian organizations
- **Critical infrastructure protection:** Security measures aligned with ACSC's Critical Infrastructure Centre guidelines to safeguard systems vital to national security and essential services
- **Threat intelligence integration:** Active incorporation of ACSC threat advisories and intelligence into our security operations and incident response capabilities
- **Essential Eight implementation:** Full deployment of the ACSC's Essential Eight mitigation strategies, which are designed to protect organizations against various cyber threats including targeted intrusions

Essential Eight Strategies

The Essential Eight is a baseline set of mitigation strategies recommended by ACSC to protect Microsoft Windows-based internet-connected networks. QuantSec has implemented all eight strategies at the appropriate maturity level:

- Application control to prevent execution of unapproved/malicious programs
- Patch applications to fix security vulnerabilities
- Configure Microsoft Office macro settings to block malicious macros
- User application hardening to reduce attack surface
- Restrict administrative privileges to prevent unauthorized access
- Patch operating systems to fix security vulnerabilities
- Multi-factor authentication to strengthen access controls
- Regular backups to ensure business continuity and data recovery

> **Compliance Details**
>
> **Alignment Status:** Fully Aligned with ACSC Guidelines
>
> **Last Review:** 2024
>
> **Essential Eight Maturity Level:** Target Level Achieved
>
> **Scope:** All QuantSec operations and service delivery

Benefits for Clients

Our alignment with ACSC guidelines provides significant benefits for our clients. It ensures that our security approach is grounded in nationally recognized best practices and informed by the latest threat intelligence from Australia's cyber security authority. This alignment is particularly valuable for organizations that need to demonstrate compliance with Australian Government security requirements or operate in sectors that are regularly targeted by sophisticated cyber threats.

Contact Information

For questions about our ACSC guidelines alignment or to discuss how our nationally-aligned security practices can benefit your organization, please contact our Compliance & Governance Team at **compliance@quantsec.com.au** or call **+61 (0)2 1234 5678**.

QuantSec Pty Ltd | Australian Cybersecurity Solutions Provider

ACSC Guidelines - Australian Cyber Security Centre Compliance

This document provides an overview of QuantSec's alignment with ACSC guidelines. For detailed security documentation, please contact our Compliance Team.

Document Version: 1.0 | Last Updated: November 2025