Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC Australian Cyber Security Centre

Overview

Gateway Security Guidance Package

First published: July 2022

Last updated: July 2025

Introduction

As cloud gateway security capabilities mature to meet enterprise customer needs, gateway architectures have evolved beyond traditional perimeter-based designs. Hybrid and cloud-native gateways, combined with new ways of working, will lead to more dynamic and distributed gateway solutions in the future.

This Gateway Guidance Security Package (the Gateway Guidance) describes how organisations should approach cyber security challenges and opportunities by embedding gateway security in their architecture. It will help them make informed risk-based decisions when designing, procuring, operating, maintaining and disposing of gateway solutions. It captures modern practices within a principle-based approach focusing on security, flexibility and adaptability across different environments. This will help organisations achieve resilient, scalable and risk-informed outcomes across diverse delivery models.

Updated gateway requirements

On 24 July 2025, the Department of Home Affairs released the 2025 update of the Protective Security Policy Framework (PSPF). This update revises gateway requirements and replaces the Australian Government Gateway Security Policy with the Australian Government Gateway Security Standard (Gateway Standard].

The Gateway Standard outlines the strategic direction for gateway use by Australian Government entities. It sets the minimum security standards that Commonwealth entities must apply when using gateway capabilities.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has updated its Gateway Guidance to align with the new Gateway Standard. These updates also incorporate recent advancements in better security practices.

Guidance for Australian organisations and service providers

The Gateway Guidance is primarily intended for Australian Government organisations and their service providers. It may also be useful for any organisation designing, procuring, operating, maintaining or disposing of a gateway.

The primary audiences across the Gateway Guidance are:

- Gateway security guidance package: Overview (this guide) is for **all audiences** before reading other guides in the package.
- Gateway security guidance package: Executive guidance is for **senior or executive decision-makers** who are accountable for designing, procuring, operating, maintaining or disposing of gateway solutions.
- Gateway security guidance package: Gateway security principles is for **security, architecture and engineering teams** who are responsible for designing or operating gateway solutions in their organisation.
- Gateway security guidance package: Gateway operations and management is for **engineering, operations and support teams** to understand better-practice approaches for operating, maintaining and disposing of gateways.
- Gateway security guidance package: Gateway technology guides is for **security, architecture, engineering, operations and support teams** and provides detailed guidance on key technical concepts referred to throughout the Gateway Guidance package.

Table 1. Primary audiences across the Gateway Guidance

Executive guidance For **senior or executive decision-makers** to help them understand their obligations and role in improving cyber security outcomes for their organisation. High-level topics: • definition of a gateway • the threat environment • requirements for government organisations	Gateway security principles For **security, architecture and engineering teams** to understand the fundamental design principles and architecture that underpin better gateway security practice. High-level topics: • key terms and concepts • gateway security principles • cloud-based gateways • visibility and telemetry • cyber threat intelligence
Gateway operations and management For **engineering, operations and support teams** to understand a better-practice approach for operating, maintaining and disposing of gateways. High-level topics: • continuous assurance and validation • secure administration • product selection • gateway maintenance • platform hardening	Gateway technology guides For **security, architecture, engineering, operations and support teams** for detailed guidance on key technical concepts referred to throughout the Gateway Guidance package. High-level topics: • evolving architecture • key gateway services (DNS, email, web proxies, reverse proxies, and remote access) • gateway threats and mitigations

Contact us

Following substantial updates to the Gateway Guidance in July 2025, ASD's ACSC welcomes feedback to ensure it remains clear, relevant and useful. If you have any questions or feedback, you can write to us or call us on 1300 CYBER1 (1300 292 371).

The Gateway Guidance is being released in parallel with the Department of Home Affairs *Australian Government Gateway Security Standard*. We encourage interested stakeholders to provide feedback on the Gateway Standard directly to the Department of Home Affairs.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre