



Australian Government

Department of Home Affairs  
Protective Security Policy Framework

# PSPF Direction 002-2025

## Kaspersky Lab, Inc. Products and Web Services

The Protective Security Policy Framework (PSPF) applies to non-corporate Commonwealth entities subject to the *Public Governance, Performance and Accountability Act 2013*. The PSPF provides that, having considered advice from technical authority entities, the Secretary of the Department of Home Affairs may issue a Direction to accountable authorities to manage a protective security risk to the Commonwealth.

The Accountable Authority of each entity must adhere to any Direction issued.

PSPF Direction 002-2025 requires Australian Government entities<sup>1</sup> to prevent the installation of Kaspersky Lab, Inc. products and web services<sup>2</sup> from all Australian Government systems and devices<sup>3</sup>, and where found, to remove all existing instances.

Further information about Kaspersky Lab, Inc. products and web services is detailed in Policy Explanatory Note 002/25 – Managing Kaspersky Lab, Inc. Products and Web services on Australian Government Systems.

After considering threat and risk analysis, I have determined that the use of Kaspersky Lab, Inc. products and web services by Australian Government entities poses an unacceptable security risk to Australian Government, networks and data, arising from threats of foreign interference, espionage and sabotage. I have also considered the important need for a strong policy signal to critical infrastructure and other Australian governments regarding the unacceptable security risk associated with the use of Kaspersky Lab, Inc. products and web services.

Entities must manage the risks arising from Kaspersky Lab, Inc.'s extensive collection of user data and exposure of that data to extrajudicial directions from a foreign government that conflict with Australian law.

By 1 April 2025, all non-corporate Commonwealth entities **must**:

1. Identify and remove all existing instances of Kaspersky Lab, Inc. products and web services on all Australian Government systems and devices<sup>3</sup>.
2. Prevent the installation of Kaspersky Lab, Inc. products and web services on all Australian Government systems and devices<sup>3</sup>.
3. Report completion of above requirements to the Department of Home Affairs' Commonwealth Security Policy Branch at [PSPF@homeaffairs.gov.au](mailto:PSPF@homeaffairs.gov.au).

<sup>1</sup> For the purposes of this Direction, 'Australian Government entities' refers to all *non-corporate Commonwealth entities that are subject to the Public Governance, Performance and Accountability Act 2013 (PGPA Act)*.

<sup>2</sup> 'Products and web services' constitutes *all information security products, solutions, and web services supplied directly or indirectly by Kaspersky Lab, Inc. or any or any of its predecessor, successor, parent, subsidiary, or affiliate companies*. This Direction does not cover other manufacturers' products that have embedded Kaspersky Lab, Inc. code.

<sup>3</sup> 'Devices' constitutes *'Government-issued mobile devices' and 'authorised non-government devices', as defined in the PSPF, which includes all mobile phones, handheld computers, tablets, laptops and personal digital assistants*.

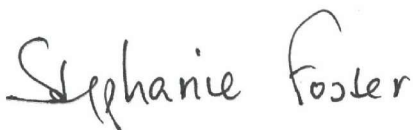
The Accountable Authority may seek an exemption for a legitimate business reason, limited to national security and regulatory functions, for the use of Kaspersky Lab, Inc. products and web services on Australian Government systems and devices<sup>3</sup> and must ensure that appropriate mitigations are in place.

Legitimate business reason is a need to install or access Kaspersky Lab, Inc. products and web services on Australian Government systems and devices<sup>3</sup> to conduct business and/or achieve a work objective of an entity. A legitimate business reason must be time limited, follow all mitigations outlined in Policy Explanatory Note 002-25 and be limited to:

- where the use is necessary for the conduct of national security or regulatory functions, including compliance and law enforcement functions.

Further information about Kaspersky Lab, Inc. products and web services, similar offerings, and appropriate mitigations for legitimate business use is detailed in Policy Explanatory Note 002-25 – Kaspersky Lab, Inc. products and web services.

For further information, contact [PSPF@homeaffairs.gov.au](mailto:PSPF@homeaffairs.gov.au) or 02 5127 9999.



**Stephanie Foster PSM**

Secretary

Department of Home Affairs

17 February 2025