

Australian Government
Department of Home Affairs

Memorandum of Understanding

on

DIGITAL RESILIENCE TO SUPPORT THE SECURITY OF AUSTRALIA

between

The Commonwealth of Australia, as represented by the Department of Home Affairs

and

Microsoft Corporation (Microsoft)

1. Purpose

1.1. This Memorandum of Understanding is entered into by Microsoft Corporation, (Microsoft) represented by Lisa Monaco, President Microsoft Global Affairs, and the Commonwealth of Australia, represented by the Minister for Home Affairs and Minister for Cyber Security.

1.2. This Memorandum of Understanding establishes a non-binding framework for strategic cooperation to strengthen Australia's digital resilience. Both parties share the imperative to protect Australia's critical infrastructure, enable secure digital transformation, and foster innovation while mitigating emerging risks. The agreement reflects a shared commitment to ensuring Australia's cloud, data, artificial intelligence, and emerging technology ecosystems remain secure, reliable and adaptable. It complements collaboration on artificial intelligence opportunities between the Australian Government and Microsoft under the National Artificial Intelligence Plan.

1.3. This cooperation is also intended to complement our shared commitment to promote open, secure, resilient, and interoperable digital ecosystems.

2. Partnership Commitments

2.1. The parties agree to collaborate under five overarching commitments:

2.2. **Annual Ministerial Meeting**

An annual meeting between the Minister for Home Affairs and the President of Microsoft Global Affairs to set direction for engagement on digital resilience.

2.3. **Annual Strategic Dialogue**

Convene one or more senior-level working groups to drive strategic alignment, policy collaboration, and whole-of-system coordination on digital resilience issues. Working groups will be empowered to set their own cadence and governance and are expected to meet at least once annually.

2.4. **Joint Initiatives for Digital Resilience**

Work together on initiatives recommended as priorities by working groups that will help to strengthen the resilience of Australia's digital technology stack and its resilience layers, including governance, platforms, foundations, cybersecurity, and supply chain security.

2.5. **Responding to Significant Technology Outages**

Work together to prioritise the recovery of Australia's digital economy as soon as possible from significant technology outages or digital disruptions within the Microsoft Corporation ecosystem, complementing established crisis-management arrangements.

2.6. **Information Exchange and Capability Building on Digital Resilience**

Facilitate structured information sharing to assist the Australian Public Service – including through the APS Academy – in upskilling its ability to interpret technology trends and developments.

3. Priority Themes for Policy Collaboration

3.1. The following six themes will guide initial areas for policy discussions and sharing of trends and developments, as the basis of ongoing cooperation. The parties will jointly determine when it is appropriate to organise a working group for each of these themes:

3.2. **Subsea Cable Resilience**

Exploring how policy alignment and adjusting to domestic and global trends and insights can enhance physical and cyber security of subsea cable infrastructure including through engagement with regional partners where appropriate.

3.3. **Data Centre Infrastructure and Hyperscale Cloud Resilience**

Support secure, scalable, and sustainable hyperscale infrastructure as a cornerstone of national resilience. Share insights on policies that improve continuity and security of cloud services critical to government and industry.

The parties agree to collaborate on resilience exercises for government and/or industry in relation to this theme.

3.4. **Regulatory Simplification**

Collaborate on frameworks that streamline compliance and promote interoperability of resilience efforts domestically and globally.

3.5. **Secure Artificial Intelligence in Government**

Share expertise to shape secure and resilient Artificial Intelligence policy and adoption across Commonwealth entities and among public sector workers, consistent with the AI Plan for the Australian Public Service.

3.6. **Small Business and Critical Infrastructure Support**

Share policies and initiatives that strengthen resilience across small and medium enterprises and critical infrastructure entities.

3.7. **Emerging threats**

Collaborate on initiatives to address new and emerging cyber security threats.

Deliverables under these themes will remain flexible and subject to agreement during the Strategic Dialogue.

4. Governance and Review

4.1. Nothing in this Memorandum of Understanding is intended to confer exclusivity or preference, or to limit the Commonwealth's engagement with other technology providers or partners.

4.2. Executive Sponsors are:

(a) For the Government of Australia, Secretary of the Department of Home Affairs.

(b) For Microsoft Corporation, the President of Microsoft Global Affairs.

4.3. A joint steering group will oversee implementation of working groups and monitor progress. The joint steering group will comprise three representatives from each party, who will be designated within 30 days after this Memorandum of Understanding is signed.

4.4. Working groups will be formed by and will make recommendations to the joint steering group.

4.5. This Memorandum of Understanding will be reviewed annually, with any amendments agreed in writing.

4.6. Where activities relate to artificial intelligence, the parties will ensure alignment with relevant whole-of-government AI governance arrangements, including those of the AI Plan for the Australian Public Service.

5. Confidentiality

5.1. All non-public information exchanged under this Memorandum of Understanding is subject to the Confidentiality terms (section 15) of the Microsoft Business and Services Agreement dated 23 January 2026 between Microsoft Ireland Operations Limited on behalf of Microsoft Corporation and all Affiliates, and the Commonwealth of Australia as represented by the Digital Transformation Agency. Public disclosure is limited to the existence and broad objectives of the Memorandum of Understanding, subject to mutual agreement.

6. Term

6.1. This Memorandum of Understanding becomes effective upon signature and will be reviewed annually. Amendments, including any extension, must be made in writing, signed by both parties. Either party may terminate this Memorandum of Understanding in its absolute discretion by providing a minimum of 30 days' written notice to the other party.