Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

14 November 2025

HUD2025-008421

s 9(2)(a)

Dear s 9(2)(a)

On 16 October 2025 Te Tūāpapa Kura Kāinga – Ministry of Housing and Urban Development (the Ministry) received your request for the following information under the Official Information Act 1982 (the Act).

The answers to your request are outlined below.

A list of all Artificial Intelligence (AI) tools that are currently approved for use by staff at your agency.

- Microsoft Copilot 365
- Oracle Fusion Cloud's AI features

Any documentation outlining the conditions, guidelines, or policies attached to the approval and use of these tools.

Three documents have been identified in scope of this request and are being released to you. Some information has been withheld under section 9(2)(a) of the Act, to protect the privacy of natural persons. The documents are detailed in the attached document schedule.

Training videos and other AI support resources are also available for all Ministry staff on its intranet.

For each approved tool that is not free to use, please provide the number of paid licenses or subscriptions the agency currently holds. I confirm that I do not require any commercially sensitive information (e.g. licence costs), merely the number of authorised users.

Both tools listed above are provided to all employees at the Ministry, approximately 320 staff.

Copies of all completed Cloud Risk Assessments and Privacy Impact Assessments (or equivalent documents) for each of the approved AI tools.

One document is in scope of this request and is being released to you. Some information has been withheld under section 9(2)(a) of the Act, and section 9(2)(k), to prevent the disclosure or use of official information for improper gain or improper advantage.

In terms of section 9(1) of the Act, I am satisfied that, in the circumstances, the decision to withhold information under section 9 of the Act is not outweighed by other considerations that render it desirable to make the information available in the public interest.

You have the right to seek an investigation and review of my response by the Ombudsman, in accordance with section 28(3) of the Act. The relevant details can be found on the Ombudsman's website at: www.ombudsman.parliament.nz.

As part of our ongoing commitment to openness and transparency, the Ministry proactively releases information and documents that may be of interest to the public. As such, this response, with your personal details removed, may be published on our website.

Yours sincerely

Emily Scarlett
General Manager, People and Community
Te Tūāpapa Kura Kāinga – Ministry of Housing and Urban Development

Annex A: Document schedule

Documents released – HUD2025-008421			
	Date	**Document**	**Section of the Act applied**
1	August 2022	Policy – Digital Acceptable Use	N/A
2	19 May 2025	Our approach to Artificial Intelligence (AI)	N/A
3	2024	Ministry Artificial intelligence (AI) Training & Guidance and security pages.	9(2)(a)
4	August 2025	Microsoft Copilot – Certification and Accreditation Memo	9(2)(a) 9(2)(k)

Policy – Digital Acceptable Use

We all access data, information and technology during our work, and we all have a responsibility to ensure we do this in an appropriate, safe and secure way.

1. Why do we have this policy?

The purpose of this policy is to ensure all HUD data, information and technology is used in the correct way and for the appropriate purpose.

It also reinforces HUD's right to monitor all use of HUD technology, systems, and information, including Bring Your Own Device (BYOD), to ensure usage is appropriate, safe and secure. Reasonable personal use of HUD technology is permitted if it does not result in unnecessary or additional costs to HUD.

2. Who does this policy apply to?

This policy applies to all HUD people who use any technology provided by HUD and/or connected to HUD systems.

3. Who has accountability or responsibility under this policy?

Role	Description of responsibility
Chief Executive	• Accountable for the ICT Acceptable Use Policy
Senior Leadership Team	• Responsible for endorsing this policy as well as promoting and supporting the continuous improvement of the acceptable use of all technology in the Ministry. • Rresponsible for receiving assurance from their managers that their group is complying with this policy and providing the Chief Executive with such assurance as necessary.

Manager, Digital and Digital Team	• Responsible for the Digital Acceptable Use Policy, including ensuring it meets the minimum requirements for development and implementation, it is signed off at the appropriate level, compliance can be monitored and breaches are investigated.
	• The Digital team will support the Manager, Digital to:
	  ○ Review the policy periodically (minimum annually) to ensure it meets HUD's requirements
	  ○ Ensure this policy is published on the Intranet and/or alternate information stores accessible by HUD people.
	  ○ Provide reporting on HUD's use of digital technology to measure compliance and investigate breaches
	  ○ Ensure this policy meets the requirements of the Government CIO and NZ Information Security Manual (NZISM).

People Team	• Ensuring all new employees and contractors receive this policy prior to starting work with HUD, and maintaining a record which confirms they have read and agreed to the policy.

4. What you must do under this policy

All our HUD People accessing HUD data, information and systems must:

- Use technology in accordance with all established policies, procedures, instructions, and guidelines for safe and secure use provided by HUD or HUD's technology partners or suppliers.
- Limit personal use of HUD technology to ensure that it does not unduly impact productivity, threaten the security of HUD's Digital environment, or negatively impact system performance and cost.
- Use only authorised and/or registered technology devices to access HUD data, information and systems.
- Manage user accounts and passwords by following instructions for safe and secure use.
- Only store HUD data and information in locations that have been approved by HUD.
- Follow HUD advice on the safe use of devices which access HUD information, data and systems by maintaining an awareness of risk, in particular when using devices in public places (e.g., cafés, public transport) or on any public Wi-Fi system (e.g., airports, hotels).
- Label, send, share and use messaging and documents appropriately, as per the rules for document classification.
- Immediately report any suspected, accidental or other breach of HUD information security or inappropriate use of technology.
- Immediately report lost or stolen devices, including BYODs, to HUD Digital or the HUD Service Desk so actions can be quickly taken to protect HUD data, information and systems.
- Not record images, audio or video unless approved by all participants and classified and stored appropriately.
- Follow the same HUD policies, procedures, instructions, and guidelines for safe and secure use when using BYOD devices to access any HUD systems or information.

All **Managers of people** must:

- Ensure their people are aware of this policy, procedures, including reminding people of their obligations under this policy.
- Discuss use of technology with their people to ensure use is appropriate, necessary, and not putting HUD at risk.
- Reinforce HUD's commitment to maximising the value realised from our investment in technology.
- Ensure the timely return of any HUD technology and information when requested or required, particularly on departure of their people.
- Review reports provided by Digital to ensure that their people have the appropriate technology allocated, are using technology appropriately, and actioning any issues.
- Ensure people receive appropriate training on how to use technology safely and securely.
- Report breaches of this policy to their manager.

5. Other Information

Definitions

Technology	For the purposes of this policy, 'technology' refers to any device or system used to produce, access, store or communicate data and information.
Appropriate Use	Reasonable and responsible use which: • is predominantly for business purposes, • does not impact on any HUD technology system performance, speed or availability, • does not incur additional or unnecessary costs to HUD, • does not involve excessive storage of personal material, • does not include any objectionable or offensive material (refer to www.cert.govt.nz – Objectionable Material for more information) • uses only HUD-approved applications and technology, • does not attempt to access or alter information that is not authorised, • is consistent with HUD's values, integrity principles and Code of Conduct.
Bring Your Own Device (BYOD)	Personally owned devices that are used to access HUD data, information and/or systems.

Related Policies & Documents

Key Polices

- Code of Conduct
- Information Management Policy
- Protective Security Policy
- Internal Privacy Policy

Key legislation, regulations and official guidelines

- Privacy Act 1993
- Official Information Act 1982
- Copyright Act 1994
- Public Records Act 2005
- Public Service Code of Conduct and Standards of Integrity and Conduct
- New Zealand Information Security Manual (NZISM)

Who to talk to for help?

For clarification about this policy in a particular situation contact the Manager, Digital.

Compliance management process and reporting

Managers are responsible for use of technology by their people. From time to time they will receive reporting from Digital to ensure that the appropriate technology is allocated, use of technology is appropriate, and costs incurred are correct.

The following compliance management tools and processes will be used to minimise the risk of breaches of this policy before they occur, allow visibility of compliance against this policy and identify trends or risks so they can be appropriately managed:

- Blocking access to websites, whitelisting applications, forcing document classification and compliance to password rules, and removing access to or applications from devices, which result in a breach of the policy.
- Tools such as checklists or online modules to help inform our people and managers of their obligations.
- Review of performance in relation to required processes, procedures or guidelines, set out in the mandatory procedures listed above, on a regular basis to ensure continued improvement.
- Breaches will be recorded in a central register.

Compliance information regarding the performance of this policy will be provided to appropriate organisational governance groups as needed.

Collection of Data

HUD will collect data related to the use of HUD information, data and technology and will use this information for the purposes of maintaining appropriate compliance, incident tracking or any other activity related to the ongoing management of all data, information and technology. This data will be retained in line with appropriate records management policies.

Training & Communication

The Digital Acceptance Use Policy is communicated to our people through the induction process, and it is available on the intranet as part of HUD's internal policies.

The Digital team will provide relevant training materials and advice.

6. Document Control

This policy is owned by HUD's People and Community team and may be revised from time to time for operational or legislative reasons. We may consult with people if a significant change to policy is being considered. Policies do not form part of an individual's employment agreement.

Owner	General Manager, People and Community
Contact	DigitalSupport@hud.govt.nz
Original Effective Date	August 2022
Review dates	August 2023 August 2024

Our approach to Artificial Intelligence (AI)

As at 19 May 2025

Introduction

This pack is designed to help you understand:

- HUD's approach to working with artificial intelligence (AI)
- your responsibilities.

The information in this pack is current as at May 2025 as we begin to deploy AI into our digital environment.

This pack is compulsory e-learning for all HUD people. Aho Learning will help us monitor who has completed this e-Learning.

Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

Government context

The New Zealand Government promotes the responsible use of AI to modernise public services and deliver better outcomes for all New Zealanders.

The Public Service Artificial Intelligence (AI) Framework:

- sets a vision for AI in New Zealand's Public Service
- defines 5 key principles to guide Public Service AI use
- outlines the policy context for Public Service AI use
- describes 6 key pillars of the Government Chief Digital Officer's (GCDO) AI work programme.

The Framework provides support for agencies in their use of AI, and how to implement these technologies safely.

HUD's use of AI aligns with this Framework.

Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

How we use AI at HUD

We use AI to improve productivity and efficiency, and to enable you to focus on more meaningful work that requires your expertise and creativity. It's not about replacing people with technology.

Over time, we expect all our people will use AI in their work.

Training, information and support will be provided to help you build your knowledge and skill in using AI.

The next pages describe:

- Our approved tools
- Your responsibilities
- Monitoring and support

Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

Approved tools

We prioritise transparency, safety and security, when selecting AI, opting for tools that are resilient and can adapt to a changing digital landscape. We consider privacy, ethics, confidentiality and data security, and we conduct thorough risk assessments and technical tests before deployment.

Currently our approved AI tools are:

- Microsoft Copilot and
- some AI functionality within Aho (Oracle).

These approved AI tools apply existing information security permissions, which means our people, financial and contractual information remain secure. These tools will only access information from the sources you already have permission to access e.g. SharePoint sites you can already see, team chats, and your personal mailbox.

The table on the next slide describes these approved AI tools at a high level, and more information is available on our AI Hub on Puna.

We'll look to incorporate more AI tools over time. We'll do this in a responsible way and we'll let you know when it happens.

Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

Approved AI tools

Tool	Description
Microsoft Copilot AI 	Microsoft Copilot is an advanced AI assistant, designed to enhance productivity and streamline workflows. Copilot works within Microsoft 365 apps like Word, Excel, PowerPoint, Outlook, and Teams, providing contextual assistance directly within these tools. Copilot can assist by summarising text, drafting emails, analysing data, brainstorming solutions, creating reports, generating creative content and automating tasks.
Aho (Oracle) AI 	Oracle is incorporating AI into its products to automate routine tasks, and to enhance productivity and user experience. Oracle's AI is designed to perform specific tasks and make decisions within a set of predetermined parameters, working with users in a conversational, adaptive manner. The tools remember previous interactions, pull from connected data sources, and generate responses tailored to each user's unique needs.

Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

Your responsibilities

You are responsible for your actions and decisions when using AI in your work.

Examples of what 'to always do'	Examples of what 'not to do'
• Always use AI in ways that aligns with our Digital Acceptable Use Policy – *'We all access data, information and technology during our work, and we all have a responsibility to ensure we do this in an appropriate, safe and secure way.'* • Always be mindful of data privacy and security, particularly when using AI to help manage personal or sensitive information • Always use your personal judgement when using AI in your work, to ensure any information generated, advice provided, or decisions made are appropriate and accurate • Always be transparent when using AI in your work, by inserting a footer or other marker into documents to inform the reader it contains AI generated information.	• Don't use unapproved AI tools on your work computer, mobile phone or any other device you use for work. • Don't rely solely on AI for your work, you're still responsible for ensuring the information generated, advice provided or decisions made are appropriate and accurate, so you need to use personal judgement when using AI in your work • Don't use AI to manipulate or deceive others, such as generating fake news, deepfakes or misleading information.

Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

Monitoring and support

Leaders will support you to use AI in your work, in a responsible way that aligns with our expectations.

We do regular checks and reporting to make sure you have the right technology to do your job and that it's being used appropriately, so we will do the same for AI tools. From time to time, we will report back to our senior leaders about how we're using AI.

Any inappropriate or unacceptable use of AI will be addressed under our Digital Acceptable Use policy and potentially our Code of Conduct.

Please visit our AI Hub on Puna for more information about our use of AI at HUD.

-->
-->

Artificial intelligence (AI)

Welcome to our AI hub where you can learn about our approach to AI, and find information, training and support to help you use AI in your work

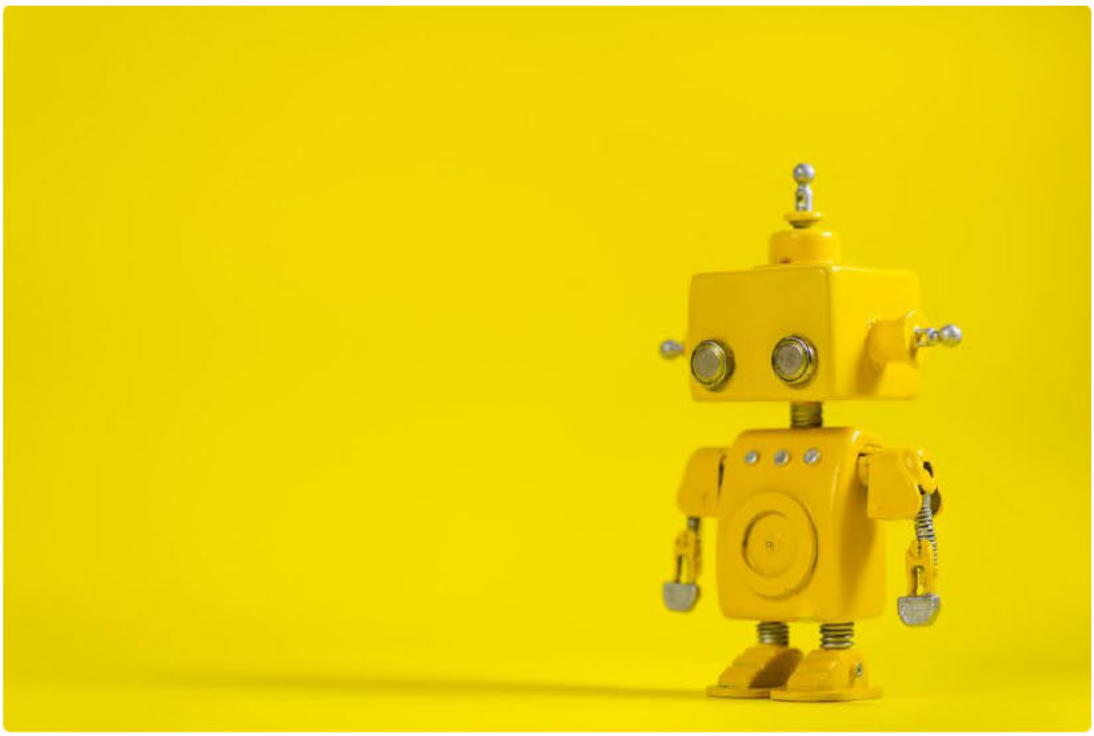
We have two approved AI tools. Microsoft Copilot AI and some functionality in Aho (Oracle).

Microsoft Copilot is an advanced AI assistant, designed to enhance productivity and streamline workflows. Copilot works within Microsoft 365 apps like Word, Excel, PowerPoint, Outlook and Teams, providing contextual assistance directly within these tools. Copilot can assist by summarising text, drafting emails, analysing data, brainstorming solutions, creating reports, generating creative content and automating tasks.

Aho (Oracle) is incorporating AI into its products to automate routine tasks, and to enhance productivity and user experience. Oracle's AI is designed to perform specific tasks and make decisions within a set of predetermined parameters, working with users in a conversational, adaptive manner. The tools remember previous interactions, pull from connected data sources and generate responses tailored to each user's unique needs.

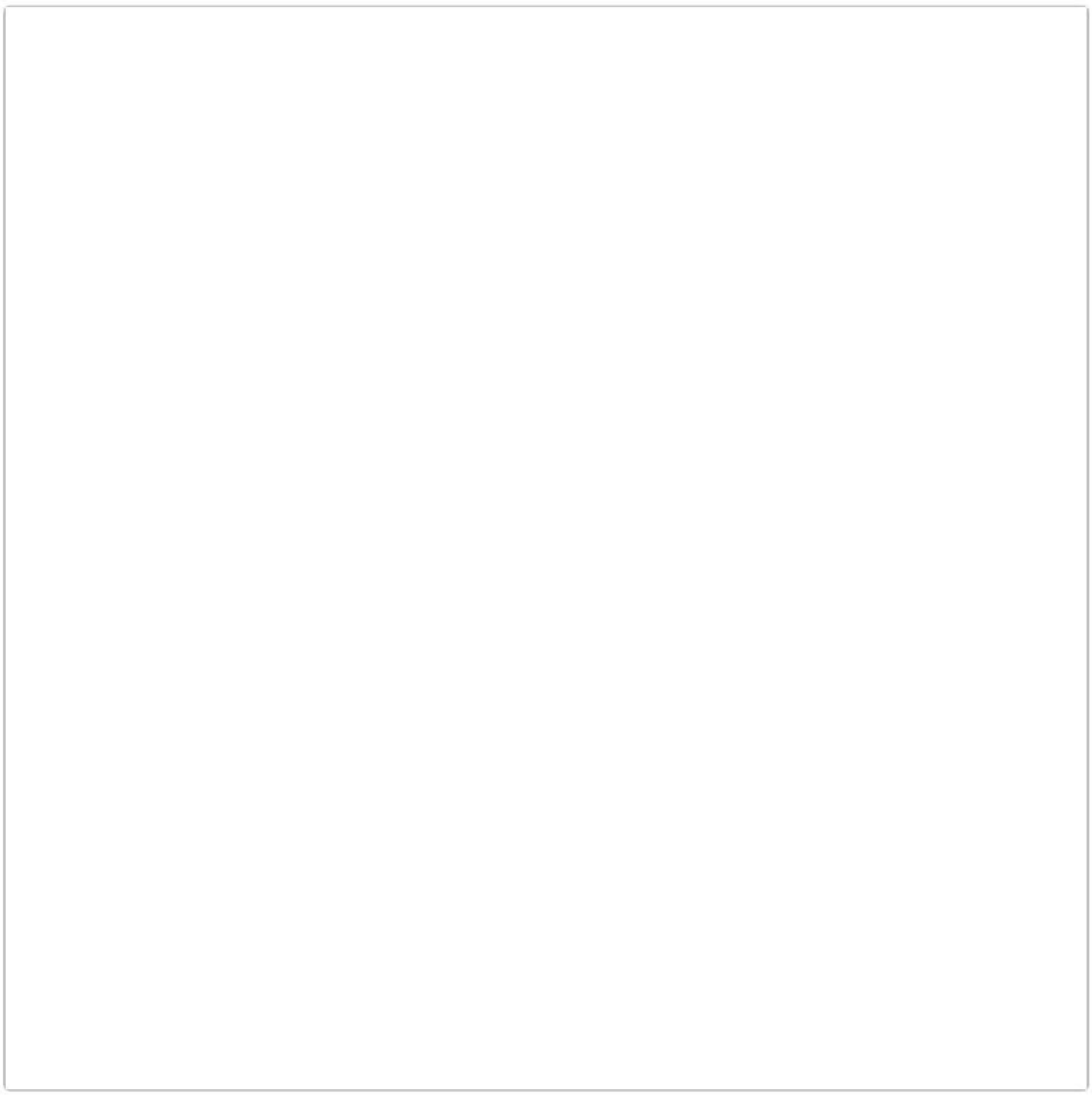
Copilot features

See what the latest features are in Copilot



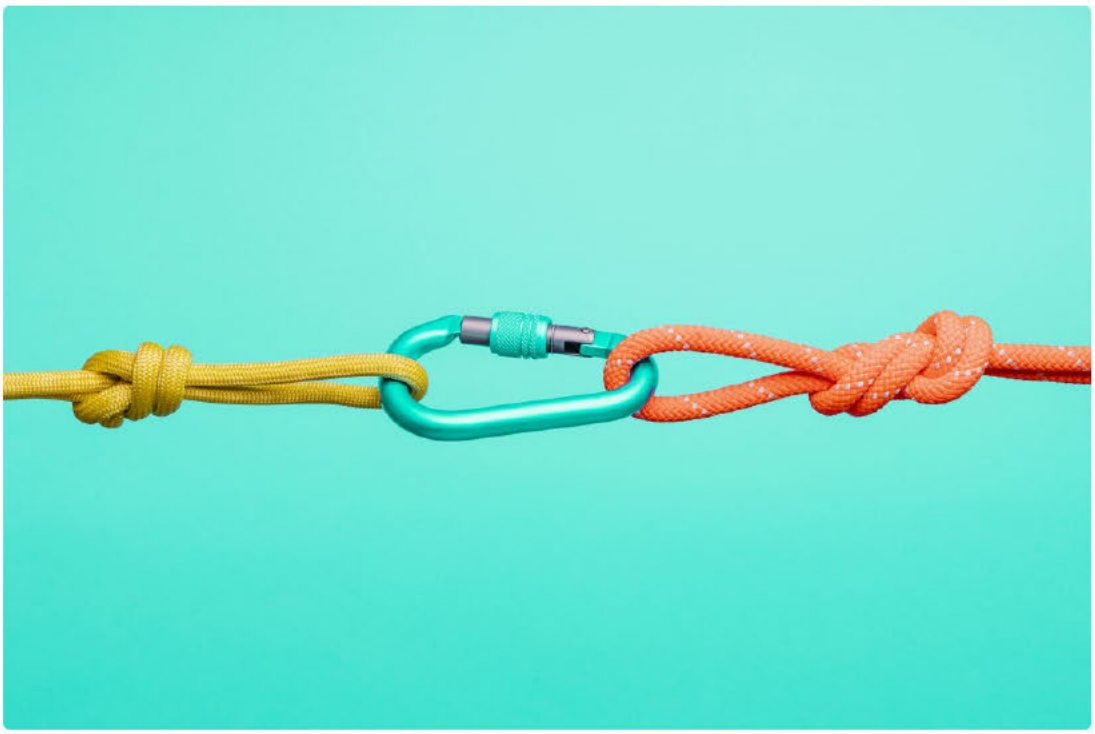
About our AI tools

Learn more about Copilot and Aho AI



Training and guidance

Learn more



Security

Learn more

Support

Learn more

Copilot roll out

Learn more

Spotted something wrong with this page?
Please contact s 9(2)(a)

View in SharePoint

How was the formatting of this email?

-->
-->

Training and guidance

On this page, you'll find information about training and guidance for using Copilot.

Learning module

We've developed a short e-learning module to describe our approach to AI, and your responsibilities. You can complete this module via Aho Learning at your own pace, ideally within two weeks of receiving access to Copilot.

Go to the self-paced learning module. When you are in Aho learning, click the 'enrol' button at the top left of your page, and then click the 'launch' button to start the course.

Microsoft 365 Copilot blog

Check out the Microsoft 365 Copilot blog, where you can:

- keep up-to-date with what's new in Copilot
- learn new ways of using Copilot and more.

Go to the Microsoft 365 Copilot blog

30-day AI journey

Take a step-by-step programme designed to help you learn the ins-and-outs of Copilot. This guided training gives you fun and easy-to-follow prompts, to help you think about how you can use them in your everyday work.

Start the great Copilot journey

Training from Microsoft

We've put together a list of easy-to-follow training that was developed for Copilot.

If you want to remind yourself about how to use our other programs like, Word, Excel or PowerPoint, head to our Digital learning hub.

Copilot in Word

Learn more

Copilot in Outlook

Learn more

Copilot in PowerPoint

Learn more

Copilot in Teams

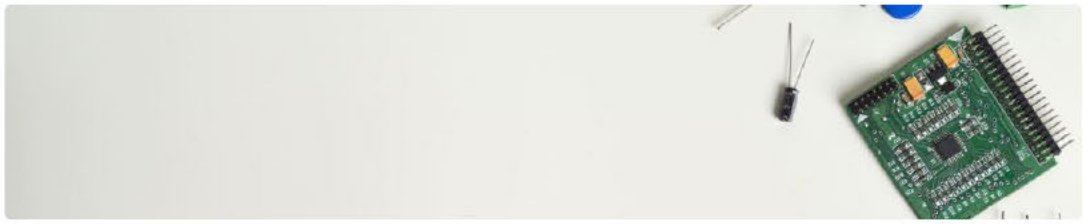
Learn more

Copilot in Excel

Learn more

Copilot prompt gallery

Learn more



Get support

Contact Digital

Spotted something wrong with this page?
Please contact s 9(2)(a)

View in SharePoint

How was the formatting of this email?

Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

-->
-->

Security

On this page, you'll find information about our expectations when you're using Copilot, our security approach, information management, digital use and privacy policy reminders.

It's important that you're mindful of how you use Copilot, including what information you ask it to generate.

Permissions

Just like our existing security measures for SharePoint, Copilot works using the same level of permissions. This means that when you ask it to generate content, it only goes looking in the areas where you already have access to.

You won't be able to ask Copilot to summarise a folder or document you don't have access to. You also won't be able to ask for sensitive information that we've blocked Copilot from accessing.

Being safe and secure

We've prioritised transparency, safety and security when selecting our approved AI tools, along with conducting thorough risk assessments and technical tests before deployment.

We've considered privacy, ethics, confidentiality and data security, and opted for resilient tools that can adapt to a changing digital landscape.

Blocking sensitive information initially

As we've completed our security assessments, we've made the decision to initially block Copilot from accessing some of the sensitive information that we look after.

For example, the commercially sensitive information that we hold about our community housing providers.

This means Copilot won't be able to access this information. If normally

have access to this information, you'll still be able to access it through Kete.

Existing internal policies

While Copilot is a new tool that you can use, it's important to remember our some of existing internal policies apply, this includes:

- Digital acceptable use policy
- Information management policy
- privacy policy
- other policies.

Make sure you familiarise yourself with the policies below.

Digital acceptable use policy

We all access data, information and technology during our work, and we all have a responsibility to ensure we do this in an appropriate, safe and secure way.

The purpose of this policy is to ensure all our data, information and technology is used in the correct way and for the appropriate purpose.

Digital acceptable use policy

Information management hub and policy

Check out our information management hub on Aho and familiarise yourself with our information management policy.

Information management hub

Information management policy

Privacy policy

Our privacy obligations still apply when using Copilot.

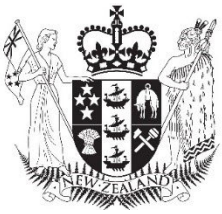
Check out the privacy services and advice Puna page

Privacy policy

Spotted something wrong with this page?
Please contact s 9(2)(a)

View in SharePoint

How was the formatting of this email?



Te Tūāpapa Kura Kāinga
Ministry of Housing and Urban Development

Te Tūāpapa Kura Kāinga – Ministry of Housing and Urban Development

Microsoft Copilot C&A Memo

Document Control

General Information

Document ID	Microsoft Copilot C&A
Document Owner	s 9(2)(a)
Issue Date	August 2025
Document Author	s 9(2)(a)
File Name	Microsoft Copilot - Certification and Accreditation Memo.docx

Revision History

Version	Date	Author(s)	Description
0.1		s 9(2)(a)	Initial Draft

Distribution List

Name	Organisation	Title
s 9(2)(a)	HUD	Acting General Manager, People and Community
s 9(2)(a)	HUD	Acting Manager, Digital & Workplace

Contents

1. EXECUTIVE SUMMARY

1.1. Introduction

The objective of this document is to recommend the interim accreditation of Microsoft CoPilot in the Azure tenancy of Te Tūāpapa Kura Kāinga – Ministry of Housing and Urban Development (HUD). This memo outlines the technical setup, high level risks, and recommendations associated with the deployment of Microsoft CoPilot (technical risks) and unique risks associated with staff adopting and using this new technology (people risks).

This memo is based on cyber security artifacts and best practice documentation from Microsoft, the National Institute of Standards and Technology (NIST), the US Cybersecurity and Infrastructure Security Agency (CISA) security guidelines, the open worldwide application security project (OWASP) top 10 AI security risks and an AI survey completed by the government chief digital officer (GCDO) in New Zealand. Two recently released draft Control Validation Plans (CVP) for AI from GCDO, based on ISO standards, were also evaluated and applied to this memo. Various other technical resources have also been used to further investigate and identify potential risks. GCDO has indicated that it is currently completing an assessment of Microsoft CoPilot as part of the Microsoft 365 yearly assessment for the DIA marketplace.

Using these security artifacts and guides listed, 18 potential risks were identified. Of these untreated risks four (4) were found to be at a high-risk level. The fourteen (14) remaining risks were assessed to be at a medium risk level.

Risk Type	Total	Low	Medium	High	Very High
Untreated	18		14	4	
Current	18	11	7		

Summary of the total number of risks (Current Assessment) at each level.

1.2. Key Points

We have reviewed the security artifacts, reviewed the configuration, and reviewed the known AI risks to confirm how they apply to the HUD CoPilot deployment, checked the existing HUD controls and their effectiveness, and identified fifteen (15) applicable controls. Most of these controls are already present in the HUD Microsoft Azure tenancy. Many of the risks identified are closely related and, in some cases, a single control could appropriately be used for more than one risk, resulting in fewer controls than risks being present. No reason was found not to continue with the certification, and no specific remediation is required because of this assessment.

Controls	Effective	Partially Effective	Not Effective	Not Assessed	Not Applicable	Total
HUD	15					15

The current HUD controls (15) have all been found to be effective and currently align risk ratings with expected residual levels. No immediate remediation activities are currently necessary.

2. CERTIFICATION & ACCREDITATION

HUD Security recommends that:

Note the current risks, Current risks, and recommendations in this report.

Note that this accreditation applies to the current versions and use cases of Microsoft CoPilot.

Auditor / Assessor

In my role as independent auditor for the Certification and Accreditation (C&A) of Microsoft CoPilot:

- I acknowledge the role and responsibility of System Auditor / Assessor.
- I confirm that the residual risk summary herein is an accurate summary of the remaining risks associated with the areas of non-compliance along with the required remediation activities, based on the Security Risk Assessment and Control Validation Audit of the Service.

I recommend the system be approved by the Accreditation Authority for operational use.

Shawn Bruwer, Assessor, HUD Security

s 9(2)(a)

Date: 15-09-2025 RECOMMENDS the use of the system for HUD.

Janine Crous, Acting Manager, Digital & Workplace

s 9(2)(a)

Date ACCEPTS the residual risks for HUD.

Devon Heaphy, Acting General Manager, People and Community

s 9(2)(a)

Date: 22/09/2025 CERTIFIES the review of the service for HUD.

Glenn Phillips, Acting Deputy Chief Executive OP (CISO)

s 9(2)(a)

Date: 7 November 2025 ACCREDITS the service for HUD

3. SOLUTION OVERVIEW

HUD Security has completed an internal review and completed this certification and accreditation memo of the Microsoft Copilot deployment being used at HUD.

Many generative AI risk frameworks are targeted at bespoke AI solutions. For the purposes of this risk assessment, HUD is adopting a fully cloud-native Software-as-a-Service (SaaS) implementation of Microsoft 365 CoPilot. All AI processing occurs within Microsoft's own environment, and the models are maintained, secured, and governed by Microsoft under the applicable Microsoft 365 terms of service, including their AI security, compliance, and privacy commitments. HUD will not be creating or hosting any AI models nor managing any underlying AI infrastructure.

3.1. Assessment Scope

The scope of the reassessment is as follows.

- Microsoft Copilot Agent

3.2. Out of Scope

- Microsoft Azure IaaS service
- Microsoft Entra ID service
- Other Microsoft 365 applications

4. INFORMATION PROFILE

4.1. Information Classification

The information stored, processed, and transmitted by the system is classified up to the level of RESTRICTED. According to the New Zealand Government Security Classification System, any disclosure of this information could potentially hinder the effective conduct of government operations in New Zealand or negatively impact the privacy of its citizens.

4.2. Privacy

A Privacy Impact Assessment (PIA) was completed by the privacy officer, and the assessment confirmed that CoPilot would optimise the use of existing personal information while maintaining the current standards of privacy and data protection at HUD. While some personally identifiable information (PII) is present, CoPilot would not introduce new information and would not be sharing information externally. Existing information includes:

- HUD Customer first and last names
- Customer contact information.
- Limited Customer financial/PCI information.
- HUD user first and last name.
- User contact information including work address and work / personal phone number

5. REVIEW DETAIL

The following steps were taken leading to accreditation:

1. Analysis of previous Certification and Accreditation (none in this case).
2. Conducted Security Risk Assessment and recommended controls.
3. Validated effectiveness of controls.
4. Remediation of ineffective controls (None Currently Required).
5. A Privacy Impact Assessment (PIA)
6. Recommended Accreditation. (Certification and Accreditation Memo)

5.1. Previous accreditation and certification

Artificial Intelligence and Microsoft Copilot are new technologies and no previous assessments exist.

5.2. Security Risk Assessment

The Security Risk Assessment was completed by reviewing security artifacts from GCDO, Microsoft, the NZISM Risk and compliance assessment and US Cybersecurity and Infrastructure Security Agency (CISA) security guidelines. The SRA identified eighteen (18) potential risks, initially rated as High (4) and Medium (14). These risks are currently successfully managed by fifteen (15) controls, which effectively reduce them to an acceptable residual risk level of medium (7) and low (11) for HUD.

5.3. Control Validation Audit

A CVA section has been added to the SRA to illustrate how the eighteen (18) risks identified by the assessment are effectively controlled by the fifteen (15) controls implemented by HUD security. Most of the risks identified are closely related and, in some cases, a single control could appropriately be used for more than one risk, resulting in fewer controls than risks being present. The HUD controls were tested and validated and where applicable, evidence was collected for audit purposes.

5.4. Remediation Activities

None required. The CVA determined that no remediation activities are immediately needed for Microsoft Copilot as all the risks identified are already effectively being controlled by the controls that have been implemented by HUD.

5.5. Current Risk Profile

To illustrate the untreated risk position and the current risk position, a risk matrix has been created for each.

Matrix 1 illustrates the comparison of untreated risks and current risks after the application of controls, providing a view of risks identified compared to a view of the risk exposure of Microsoft Copilot after the confirmation of the effective controls HUD have implemented to mitigate the untreated risks.

The untreated risks were previously noted at a **Medium to High** risk level (overall) and the current risks are now rated at a **Medium to Low** risk level demonstrating a significant improvement to the risk position.

6. Untreated vs Current Risk

Impact	Untreated Risk						Current Risk				
	15	19	22	24	25	Severe	15	19	22	24	25
	10	14	18 AIR-P01 AIR-P05 AIR-T01 AIR-T02	21	23	Significant	10 AIR-T01	14	18	21	23
	6	9 AIR-P06 AIR-T05 AIR-T06 AIR-T07 AIR-T08 AIR-T09	13 AIR-P02 AIR-P04 AIR-T03 AIR-T04 AIR-T11 AIR-T12	17	20	Moderate	6	9 AIR-T02	13	17	20
	3	5 AIR-T10	8 AIR-P03	12	16	Minor	3 AIR-P02 - AIR-P03 AIR-P04 - AIR-P05 AIR-P06 - AIR-T05 AIR-T06 - AIR-T07 AIR-T08 - AIR-T09 AIR-T10	5 AIR-P01 AIR-T03 AIR-T04 AIR-T11 AIR-T12	8	12	16
	1	2	4	7	11	Minimal	1	2	4	7	11
	Almost Never	Possible but Unlikely	Possible	Highly Probable	Almost Certain		Almost Never	Possible but Unlikely	Possible	Highly Probable	Almost Certain
	Likelihood										

Matrix 1- Untreated vs Current risks

7. SUMMARY OF FINDINGS

A total of eighteen (18) risks and fifteen (15) controls were deemed relevant to the application. The risks have been subdivided into **People Risks** and **Technology Risks.**

The following table outlines the untreated cybersecurity risks identified along with current controls already being enforced by HUD to protect and secure CoPilot. The Risk level before (Untreated risks) indicates the risk to HUD prior to effective controls being put in place. The Risk level now (Current risk) indicates the much-improved risk position after HUD implemented controls already in use. An audit has been conducted to assess these controls and their effectiveness at reducing risk to achieve the target risk levels. See the HUD Control Matrix in this document for a more granular explanation of controls listed in the table below.

7.1 People Risks

Risk ID	Name	Risk Description	Risk level Before	HUD Controls already in use	Risk level now
AIR-P01	**Insufficient Role based training for using CoPilot**	Insufficient role based training for using CoPilot could lead to employees carrying out insecure practices or accidental exposure of confidential information.	**HIGH (18)**	**C14 Role-Based Training** **C47 Documentation** **C49 Data Governance** HUD controls are effective and adequate currently.	**MEDIUM (5)**
AIR-P02	**Risk of insider threat (Amplification)**	Authorised users may misuse their access to confidential information. A malicious insider could misuse AI to create scripts, or shadow IT programs to gain access to confidential information / restricted areas or to deliberately bypass important governance or security processes.	**MEDIUM (13)**	**C01 Access Control** **C02 User Lifecycle Management** **C14 Role-Based Training** **C36 Logging, Monitoring and Alerting** HUD controls are effective and adequate currently.	**LOW (3)**
AIR-P03	**Risk of Inaccurate Content Generation and usage**	AI may hallucinate or fabricate information. This occurs when CoPilot produces output that appears plausible but is factually incorrect, unverifiable, or entirely fabricated. CoPilot's answers may lack empathy if used in difficult or personal conversations with staff.	**MEDIUM (8)**	**C14 Role-Based Training** **C49 Data Governance** HUD controls are effective and adequate currently.	**LOW (3)**
AIR-P04	**Risk of Shadow IT usage of CoPilot**	Shadow IT refers to technology systems, applications, and services used or created by staff without explicit HUD Digital approval or oversight.	**MEDIUM (13)**	**C14 Role-Based Training** **C36 Logging, Monitoring and Alerting** HUD controls are effective and adequate currently.	**LOW (3)**

Risk ID	Name	Risk Description	Risk level Before	HUD Controls already in use	Risk level now
AIR-P05	**Risk of Service Desk Overload**	New tools may increase support demands. Service desks and support staff may experience and overload of end users requiring help or guidance. Microsoft CoPilot especially in a government setting, is often a steep learning curve for end users and the use of AI in a daily work context can be overwhelming, especially as the use of AI is being heavily encouraged by the New Zealand government.	**HIGH (18)**	**C14 Role-Based Training** **C25 Performance and Capacity Management** **C47 Documentation** **C14 Role-Based Training** **Note:** HUD has appointed "CoPilot champions" in each business team to reduce the load on IT. HUD controls are effective and adequate currently.	**LOW (3)**
AIR-P06	**Risk of Copyright Infringement**	HUD users may unknowingly use or distribute copyrighted material suggested by Microsoft CoPilot as it uses can use vast amounts of publicly available and licensed content, on the internet and copyrighted material saved to SharePoint that can be accessed by CoPilot.	**MEDIUM (9)**	**C14 Role-Based Training** **C49 Data Governance** HUD controls are effective and currently adequate. **Note:** Microsoft has publicly indemnified its customers from copyrighted material being re-created by CoPilot publicly.	**LOW (3)**

Technical Risks

Risk ID	Name	Risk Description	Untreated Risk level	Recommendation and Controls	Risk level now
AIR-T01	**Risk of Unauthorized Access**	A malicious person may gain unauthorized access to the HUD infrastructure tenancy and as Microsoft CoPilot will have default access to most parts of the HUD tenancy and storage and can be used to expedite searches, summaries, creating reports.	**HIGH (18)**	**C02 User Lifecycle Management** **C03 Privileged Access Management** **C05 Role-Based Access Control** **C09 Multi-Factor Authentication** **C49 Data Governance** **C36 Logging, Monitoring and Alerting** HUD controls are effective and currently adequate.	**Medium (10)**
AIR-T02	**Risk of Insecure Configuration**	Microsoft CoPilot is deeply integrated into the HUD Microsoft 365 tenancy. CoPilot relies on the configuration of: **Entra ID:** for identity, authentication, access control **SharePoint / OneDrive / Teams:** for data access **Microsoft Purview:** for data governance (sensitivity labels, retention, DLP) **Microsoft Defender / Sentinel:** for monitoring If any of these components are misconfigured, Microsoft CoPilot may inherit overly permissive access or missing enforcement of governance controls. Microsoft CoPilot itself is completely secure but incomplete / misconfiguration will expose too much information.	**HIGH (18)**	**C23 Architecture Design and Review** **C29 Change Management** **C30 Configuration Management** **C36 Logging, Monitoring and Alerting** **C49 Data Governance** HUD controls are effective and currently adequate.	**MEDIUM (9)**

Risk ID	Name	Risk Description	Untreated Risk level	Recommendation and Controls	Risk level now
AIR-T03	**Risk of Insufficient Logging, Monitoring and Alerting**	Microsoft CoPilot operates within the Microsoft 365 environment, using user identity and permissions. However, most CoPilot actions are not explicitly logged as "CoPilot or AI actions." This includes: What prompt the user issued What CoPilot responded with Which documents/emails/data have referenced. If the AI output was shared, forwarded, or altered If logging and alerting systems do not account for AI-specific behaviors, misuse, data leakage, or compliance violations may go unnoticed.	**MEDIUM (13)**	**C36 Logging, Monitoring and Alerting** **C49 Data Governance** HUD controls are effective and currently adequate.	**MEDIUM (5)**
AIR-T04	**Data Leakage via AI Prompts**	Data leakage via prompts occurs when users include confidential, sensitive, or regulated information in the prompts they send to Microsoft CoPilot (or any AI interface). Although Microsoft CoPilot operates within a secure Microsoft 365 environment and does not transmit data to public LLMs like ChatGPT, data included in prompts may still be exposed within your tenant through: Accidental access by other users (draft including prompt is saved or shared) Generated content containing sensitive material unintentionally surfaced or forwarded Summaries that extract information from files the user can access but didn't intend to share	**MEDIUM (13)**	**C14 Role-Based Training** **C36 Logging, Monitoring and Alerting** **C49 Data Governance** HUD controls are effective and currently adequate.	**MEDIUM (5)**
AIR-T05	**Lack of Transparency in CoPilot Decisions**	Microsoft CoPilot suggestions may not always cite clear sources. Microsoft CoPilot uses large language models (LLMs) that generate content based on statistical patterns rather than deterministic rules.	**MEDIUM (9)**	**C14 Role-Based Training** **C36 Logging, Monitoring and Alerting** **C49 Data Governance** HUD controls are effective and currently adequate.	**LOW (3)**

Risk ID	Name	Risk Description	Untreated Risk level	Recommendation and Controls	Risk level now
AIR-T06	**Risk of Accidental Exposure of Confidential Information**	Microsoft CoPilot may generate content based on historical access to sensitive data as it does not inherently know which documents are confidential unless: Documents are properly classified/labeled using Microsoft Purview sensitivity labels Access controls and role-based permissions are tightly enforced in Microsoft 365 Information barriers are implemented to segment departments or roles	**MEDIUM (9)**	**C02 User Lifecycle Management** **C05 Role-Based Access Control** **C14 Role-Based Training** **C29 Change Management** **C49 Data Governance** HUD controls are effective and currently adequate.	**LOW (3)**
AIR-T07	**CoPilot May Have Over Permissive Access**	The Microsoft CoPilot agent may have levels of system access that enables access to information through user prompts that it should not have access to. CoPilot will inherit the same access as the user account, often with no additional restrictions.	**MEDIUM (9)**	**C01 Access Control** **C02 User Lifecycle Management** **C05 Role-Based Access Control** **C29 Change Management** **C49 Data Governance** HUD controls are effective and currently adequate.	**LOW (3)**
AIR-T08	**Risk of Inadequate or No Audit Trail for CoPilot Activity**	Actions by CoPilot may not be logged or attributed clearly. CoPilot interacts with user data, generates content, and performs actions, but by default does not log full details of activities in a traditional, auditable format. This results in inadequate Audit trails and Poor forensic investigation capability.	**MEDIUM (9)**	**C36 Logging, Monitoring and Alerting** **C49 Data Governance** HUD controls are effective and currently adequate.	**LOW (3)**
AIR-T09	**Prompt Injection Attack Risks**	Prompt injection is a manipulation technique where an attacker crafts an input prompt that alters the behavior of a language model (LLM), tricking it into ignoring or modifying instructions, disclosing sensitive data, or executing unintended actions. **Direct Prompt Injection** - a prompt or message that overrides system instructions **Indirect Prompt Injection** - model is manipulated by user content that contains hidden or malicious prompts.	**MEDIUM (9)**	**C05 Role-Based Access Control** **C14 Role-Based Training** **C43 Secure Application Development** **C36 Logging, Monitoring and Alerting** **C49 Data Governance** HUD controls are effective and currently adequate.	**LOW (3)**

Risk ID	Name	Risk Description	Untreated Risk level	Recommendation and Controls	Risk level now
AIR-T10	**Risk of Vendor Lock In**	Heavy reliance on Microsoft CoPilot may reduce tool diversity. Vendor lock-in occurs when an organization becomes dependent on a single provider (Microsoft, in this case) for technology and services	**MEDIUM (5)**	**C18 Exit Strategy** **C23 Architecture Design and Review** HUD controls are effective and adequate currently. HUD is also investing in Oracle Fusion Cloud AI tools.	**LOW (3)**
AIR-T11	**Risk of Regulatory and Compliance Gaps**	AI use may violate privacy rules. Microsoft CoPilot operates by accessing, processing, and generating content based on organizational data including emails, documents and chats. While Microsoft provides strong baseline security and privacy protection, CoPilot introduces areas of risk that existing compliance frameworks may not cover.	**MEDIUM (13)**	**C36 Logging, Monitoring and Alerting** **C49 Data Governance** HUD controls are effective and adequate currently.	**MEDIUM (5)**
AIR-T12	**Risk of Cross Tenant Data Exposure**	Cross-tenant data exposure occurs when data from your Microsoft 365 tenant is inadvertently or improperly accessed, processed, or shared with: External organizations (other Microsoft 365 tenants) Third-party services connected via Graph API or plugins Microsoft services that may process data across regions or tenants	**MEDIUM (13)**	**C05 Role-Based Access Control** **C36 Logging, Monitoring and Alerting** **C49 Data Governance** HUD controls are effective and adequate currently.	**MEDIUM (5)**

8. HUD CoPilot Control Matrix

ID	Control Title	Status	Control Description
C01	Access Control	Effective	As per Microsoft best practice, all access using Entra ID follows the least privilege rule and an Access review was completed to limit Copilots access.
C02	User Lifecycle Management	Effective	HUD Monthly access reviews are conducted and integrated into the onboarding and offboarding processes. Access is strictly Role-Based and aligned with the principle of least privilege. When users transfer between departments, their access is updated by transitioning them between the appropriate Entra groups based on their new role. This ensures that data access remains limited to what is necessary, particularly since CoPilot inherits user permissions.
C03	Privileged Access Management	Effective	By default, Microsoft CoPilot inherits the same permissions as the user. s 9(2)(k)
C05	Role-Based Access Control	Effective	Prevent Microsoft CoPilot from accessing data across certain departmental or role boundaries (Information barriers)
C09	Multi-Factor Authentication	Effective	Multi Factor Authentication (MFA) is required a s 9(2)(k)
C14	Role-Based Training	Effective	Extensive role-based general training for CoPilot was conducted prior to and during deployment at HUD. Users were trained to treat CoPilot output as draft content requiring manual validation before use or publication. Staff are aware of AI hallucination risks, such as fake citations and vague references and are encouraged to identify, flag, and report these directly within CoPilot. This general training covers many of the security and privacy awareness topics that new users of AI agents and CoPilot may be facing in their daily tasks. The CoPilot training is complimented by the online training material already available to HUD users.
C18	Exit Strategy	Effective	s 9(2)(k)
C23	Architecture Design and Review	Effective	A Microsoft 365 tenant configuration assessment and review were completed by the HUD Cloud Administrator in preparation for this rollout that focused on identity, access, data governance, and security controls affecting CoPilot visibility.
C25	Performance and Capacity Management	Effective	HUD does use analytics (Defender, Dynamics, Purview.) to monitor and scale support by identify surges and allocate resources dynamically.
C29	Change Management	Effective	HUD's Microsoft CoPilot deployment followed a staged approach, beginning with low-risk departments validating configuration controls. Training and quick reference guides supported the rollout. Deployment to sensitive areas such as Legal, HR, and Finance was intentionally delayed until HUD Digital was confident that risks had been sufficiently mitigated.
C30	Configuration Management	Effective	HUD has used international and regional standards and guidance and best practice to complete this deployment. A readiness review was completed, and many security artifacts were used to confirm that the HUD deployment would be secure and that our Access control would be adequate.
C36	Logging, Monitoring and Alerting	Effective	s 9(2)(k)
C43	Secure Application Development	Effective	For any AI-generated code, enforce checks (Development Guidance) for license compatibility before integration
C47	Documentation	Effective	Clear, practical Microsoft CoPilot usage guides are available for HUD users. HUD has developed and distributed quick reference guides for common CoPilot issues.
C49	Data Governance	Effective	HUD does have an acceptable use policy of digital systems, controlling AI-specific guidance. Users are encouraged to acknowledge AI-generated content to distinguish it from human-created work. Users are also encouraged to not blindly accept content generated by AI. HUD also enforces auto-classification of information and applies retention policies across all data stores.

9. PSR REVIEW

PSR Mandatory Requirements				
Governance	**GOV1**	**GOV2**	**GOV3**	**GOV4**
	Correct Governance	**Risk Based Approach**	**Business Continuity**	**Security Awareness**
Status:	Pass	Pass	N/A	Pass
Governance	**GOV5**	**GOV6**	**GOV7**	**GOV8**
	Manage Risks	**Manage Security Incidents**	**Respond to threat levels**	**Assess capability**
Status:	Pass	Pass	Pass	Pass
Information security	**INFOSEC1**	**INFOSEC2**	**INFOSEC3**	**INFOSEC4**
	Need to protect	**Information Security**	**Validate Controls**	**Up to date Security**
Status:	Pass	Pass	Pass	Pass

10. HUD CONTROL CATALOGUE

Refer to control catalogue found here.

11. RISK DEFINITIONS

More information about the risk escalation, reporting, likelihood and impact assessment can be found here.