

## Executive Summary

This document outlines comprehensive guidelines for the responsible use of Artificial Intelligence (AI) within BITS Technology Group, ensuring alignment with cybersecurity best practices, data protection regulations, and client confidentiality standards. The policy aims to foster a secure, compliant environment while promoting ethical AI utilisation.

## Purpose

The primary purpose of this policy is to establish clear guidelines for the responsible integration and use of AI tools within the organisation. By adhering to these guidelines, BITS Technology Group ensures compliance with cybersecurity best practices, data protection regulations, and client confidentiality standards. These include Australian Privacy Principles (APPs) and Notifiable Data Breaches (NDB) Scheme. This policy also aims to mitigate risks associated with AI usage, ensuring that all activities are conducted ethically and securely.

## Scope

This policy applies to all employees who utilise AI tools in the execution of their duties at BITS Technology Group. It covers both internal work-related functions and client-related tasks, emphasizing the importance of integrating AI responsibly into business processes without compromising data security or confidentiality.

## AI Tools and Their Permitted Uses

### Approved AI Tools

#### Microsoft CoPilot with EDP - [Free](#) and [Licensed](#)

##### Internal Use Cases:

- Enhancing meeting transcription accuracy.
- Assisting in searching for internal documents, such as reports and correspondence.
- Generating summaries of internal communications to streamline reporting.
- Email sentiment amendment and proofreading
- IT support assistance

#### BITS Local Hosted AI

##### Internal Use Cases:

- Supporting the preparation of Statement of Works (SOWs) for projects by automating data extraction and analysis.
- Facilitating coding and PowerShell scripts to manage client-related tasks efficiently.
- Handling documents containing sensitive client information, ensuring secure processing.
- Sanitising documents with sensitive material

These AI tools will be available for use by heading to <https://myapps.microsoft.com/>. You must be signed in with your BITS Microsoft Account to use these tools.

### Prohibited AI Usage

**Data Security:** No client data shall be uploaded to any AI tool other than Microsoft CoPilot with EDP and BITS Local Hosted AI without explicit approval from IT Security and Management.

**Unauthorised Use:** Employees are prohibited from using public or cloud-based AI solutions (e.g., ChatGPT, Google Gemini) for work-related tasks. Such activities must require prior written consent from IT Security and Management.

## Cybersecurity and Data Protection

#### Content Review

- AI-generated content must undergo thorough review to identify and mitigate security risks before deployment or distribution. Please see your manager for approval.

#### Data Handling

- Client data processed by AI must remain within the company's secure environment, complying with applicable data protection regulations (e.g., APP and NDB). Specific encryption standards and access controls shall be adhered to as per current BITS cybersecurity policies.

#### Input Protection

- Employees must refrain from inputting sensitive credentials or security-sensitive information into AI tools. This includes avoiding the use of personal accounts for internal work processes that require sensitive data entry.

#### Compliance with Policies

- AI usage must align with internal BITS cybersecurity policies, including access control mechanisms and audit logging practices. Regular audits by the BITS Security team will ensure adherence to these standards.

## Compliance and Enforcement

**Disciplinary Action:** Violations of this policy may result in disciplinary action.

**Audit Conduct:** The BITS Security team will conduct periodic audits to assess compliance with the policy and identify areas for improvement.

**Incident Reporting:** Any suspected or confirmed security incidents related to AI usage must be promptly reported to the BITS Security team.

## Review and Updates

This policy will undergo annual reviews, as well as updates whenever significant changes in AI technology, cybersecurity threats, or regulatory requirements emerge. The BITS leadership team will

collaborate with other departments to ensure that the policy remains relevant and robust against evolving challenges.

# Training and Awareness

A dedicated training session will be implemented to educate employees on proper AI usage practices. This initiative aims to enhance awareness of the policy's objectives and risks, ensuring a collective commitment to ethical and secure AI utilisation.

## Version Control

This document is subject to updates. The version number will be included in the effective date of future revisions for reference.

By adhering to this policy, BITS Technology Group commits to fostering an environment where AI utilisation is both effective and secure, contributing to the company's growth and operational excellence.

# AI Risk Assessment Matrix

Risk Category	Risk Description	Likelihood	Impact	Mitigation Strategies
Data Privacy	Unauthorised AI tool processes client data	Medium	High	Restrict AI use to BITS Local Hosted AI; enforce access controls.
Security Breach	AI-generated content leaks sensitive information	Low	High	Implement security audits, enforce data encryption.
Regulatory Non-Compliance	AI usage violates data protection laws (Privacy Act 1988)	Medium	High	Align AI use with Australian Privacy Principles (APPs); conduct compliance training.
Bias & Ethics	AI-generated outputs exhibit unintended bias	Low	Medium	Regularly review AI-generated content for fairness and accuracy.
Data Integrity	AI-generated scripts introduce errors or vulnerabilities	Medium	High	Review all AI-assisted code before deployment; perform security testing.
Employee Misuse	Staff uploads unauthorised data to public AI tools	Medium	High	Provide AI usage training; enforce strict policies with monitoring.

# References

[Data, privacy, and security for web search in Microsoft 365 Copilot and Microsoft 365 Copilot Chat](#)

[Enterprise data protection in Microsoft 365 Copilot and Microsoft 365 Copilot Chat](#)

[Australian Privacy Principles](#)

[Notifiable Data Breaches](#)