



Artificial Intelligence (AI) Use, Detection and Prohibition Policy

Published & Effective: 28/03/2024

TABLE OF CONTENTS

1.	APPLICATION	2
2	EFFECTIVE DATE: 30/11/2023.....	2
3	POLICY IMPLEMENTATION, APPROVAL, MONITOR AND REVIEW.....	2
4	PURPOSE AND DEFINITION.....	2
5	SUCON AI GUIDING PRINCIPLES	3
6	PROHIBITED USE	3
6.1	AI and Plagiarism	4
7	SECURITY MEASURES AND AI DETECTION.....	4
7.1	Ways We Check For AI Usage	4
7.2	Financial Usage	5
8	RED FLAGS AND CHARACTERISTICS OF CORRUPTION.....	5
9	REPORTING PROCESS AND PROCEDURES.....	5
9.1	Non-Compliance	5
9.2	Appeal Process.....	6
9.3	Whistle Blower Protection and Retaliation Prevention	6
13.	POLICY FEEDBACK.....	6

1. APPLICATION

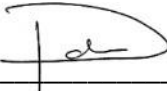
This policy applies to all paid, contracted and volunteering staff of the Sucon Consultancy Ltd (from here on referred to as 'Sucon'. This policy also applies to all Sucon associates, subcontractors and freelancers. This policy also extends to all business extensions of Sucon.

2 EFFECTIVE DATE: 30/11/2023

This applies to all Sucon relevant operations from the effective date stipulated above. From the date stipulated above all previous policy and practices are repealed.

3 POLICY IMPLEMENTATION, APPROVAL, MONITOR AND REVIEW

The Central Administration and the responsible officer(s) of Sucon via the authority of the President, Vice President and Operations Manager are liable for the management and implementation of this policy and ensuring that its provisions and records management are applied and adhered to. This includes the establishment of relevant record-keeping systems.

APPROVAL AND REVIEW	DETAILS
Policy Author	Eric Clem Groves, Vice President
Council Approval	 Lefaotogi Paletasala Faolotoi President
Next Review Date	March 2027

4 PURPOSE AND DEFINITION

The exploration and use of Generative AI / Open AI / Chat GPT tooling (from this point forward referred to as Generative (AI) by employees of Sucon Consultancy Ltd is permitted and in fact encouraged for work-related purposes. Generative AI is a new, exciting, and powerful tool that can assist in various aspects of work, including but not limited to writing, research, analysis, and customer service. At Sucon Consultancy Ltd, we embrace new technologies and encourage our teams to leverage them to improve efficiency and effectiveness, and enable the achievement of our objectives. However, it is vitally important that employees use Generative AI responsibly while remaining compliant with all existing company policies and all applicable laws.

We are committed to providing a safe and secure environment for our employees, partners, and customers and this includes our responsible use of Generative AI tooling. This policy outlines the guidelines and principles that employees must follow when using Generative AI capabilities. The company developed these guidelines so that we can experience the benefits of Generative AI tooling while ensuring its utilization is secure and aligned with our expectations for conduct and our internal data privacy controls.

Once PRINTED, this is an UNCONTROLLED document. Please email info@sucon.ws for latest version.

5 SUCON AI GUIDING PRINCIPLES

The Sucon recognises that this Policy serves both the public good, in line with the Council's commitment to social responsibility, and the Sucon interests in maximising the potential impact of our services. Sucon's AI Principles are as follows:

a) Generative AI should be used to assist employees in their work, not perform their work.

This means that the company has determined that all current policies apply to an employee's use of Generative AI, including but not limited to the Employee Proprietary Information Agreement, as well as all company policies pertaining to confidential information; intellectual property; bias, harassment, and discrimination; fraud and other illegal activities.

b) All existing company policies apply to the utilization of Generative AI.

This means that all policies such as Anti-corruption, plagiarism apply to the application and use of AI.

6 PROHIBITED USE

While Sucon Consultancy Ltd allows and encourages utilization of Chatbots/Large Language Models (LLMs) such as ChatGPT, autonomous AI agents including but not limited to AutoGPT, Godmode AI, and AgentGPT are not by default approved for company use. Due to the functionality, failure modes, and risks associated with autonomous AI agents, utilization is prohibited unless a request is made and approved by the Vice President, Engineering and the Executive Leadership Team. As of the writing of this policy, Sucon does not permit the use of Generative AI in the candidate selection process in any way that would replace or substantially assist in the decision-making responsibilities of our hiring teams. Prohibited use of Generative AI includes but is not limited to screening or comparing candidate data, profiles, or resumes. Generative AI may be used to assist with various components of the recruitment process such as assisting with the drafting job description language and suggesting potential interview questions.

As of the writing of this policy, Sucon does not permit the use of Generative AI to directly communicate or interact with any other person through bots or any similar technology. Generative AI may be used to assist with drafting or editing of communications but may not be used for direct communication with others internal or external to Sucon. As previously stated in this document, all current policies apply to the utilization of Generative AI. For the purposes of reinforcing this expectation, we are providing the following illustrative examples of activities that are strictly prohibited and constitute serious violations of company policy. These following will result in disciplinary action, up to and including termination of employment.

- a) Sharing company confidential and proprietary information in a Generative AI chat or by any other means sharing or entering this information into a Generative AI tool.
- b) Sharing customer or partner confidential information in a Generative AI chat or by any other means sharing or entering this information into a Generative AI tool.
- c) Sharing Personally Identifiable Information (PII) in a Generative AI chat or by any other means sharing or entering this information into a Generative AI tool.
- d) Using Generative AI in a way that is not professional and respectful of other including using Generative AI to engage in any form of discrimination, harassment, or other

Once PRINTED, this is an UNCONTROLLED document. Please email info@sucon.ws for latest version.

inappropriate behavior.

- e) Using Generative AI to engage in any activity that violates Sucon's policies.
- f) Using Generative AI to engage in illegal activity, including but not limited to fraud, intellectual property theft, and copyright infringement.

For clarity, entering confidential information into the tool is prohibited without regard to how the information is shared. The means of sharing may include, but is not limited to, direct entry, copying and pasting, uploading, video, voice, or any other means of sharing. Further, entering confidential information is prohibited whether or not the entry is saved. Only information that is generally publicly available may be entered into Generative AI tooling. If employees are unsure about whether or not information is confidential, they are expected to ask a member of the People or Legal team prior to sharing such information Generative AI.

6.1 AI and Plagiarism

Plagiarism is the act of using someone else's ideas, words, images, creative works, or intellectual property without giving appropriate credit or authorisation. The use of AI for original and official published company work, or article submissions to the Pacific Projects Digest are prohibited.

7 SECURITY MEASURES AND AI DETECTION

Utilisation of Generative AI for any work-related purpose should always be done through an account associated with an employee's sucon.ws email address rather than a personal email address. As with any system that is used by Sucon employees, those using Generative AI must ensure that their login credentials are kept confidential and not shared with anyone. In case an employee suspects any breach of security or unauthorized use, they must report it immediately to a member of the Presidents Council.

It is mandatory when supervisors cross check employee submissions and work, company approved and procured AI detection tool must be used. The use of AI cannot exceed 50% of the generated work by employees. AI detection of more than 50% will be returned to be reproduced by the employee.

7.1 Ways We Check For AI Usage

- a) **Plagiarism Detection Software:** Utilise plagiarism detection tools to identify similarities between submitted assignments and known AI-generated content.
- b) **In-Depth Evaluation:** Review assignments for inconsistencies in writing style, unusual vocabulary, or unnatural language patterns that may indicate AI usage.
- c) **Individual Assessments:** Design assignments and work that are tailored to each employees understanding and require personalised responses, making it difficult for AI-generated content to fulfil the criteria.
- d) **Verbal Defense:** In some cases, conduct oral assessments to allow staff to explain their tasks and assignments and demonstrate their understanding of the topic.
- e) **Knowledge-Based Questions:** Include questions in assignments that require staff to apply their knowledge beyond the scope of readily available AI-generated information.
- f) **Randomised Elements:** Introduce randomised elements or scenarios that prevent staff from relying solely on pre-existing AI-generated materials.
- g) By **implementing this policy** and employing effective detection methods, Best Practice Network can ensure a fair and genuine learning environment that promotes intellectual growth and academic excellence.

7.2 Financial Usage

At present, there are free Generative AI tools available that are sufficient to allow for the utilization outlined in this policy. The company will not pay for or reimburse employees for premium subscriptions or other costs associated with Generative AI tooling. A business case for an exception request will require the approval of the Vice President, Engineering and the Executive Leadership Team.

8 RED FLAGS AND CHARACTERISTICS OF CORRUPTION

The following is a list of red flags that may indicate the possible existence of corrupt practices and should be kept in mind by all those subject to this Policy:

- a) Use of an agent with a poor reputation or with links to a foreign government.
- b) Unusually large commission payments or commission payments where the agent does not appear to have provided significant services.
- c) Cash payments, or payments made without a paper trail or without compliance with normal internal controls.
- d) Unusual bonuses to foreign personnel for which there is little supporting documentation.
- e) Payments to be made through third-party countries or to offshore accounts.
- f) Private meetings are requested by public contractors or companies hoping to tender for contracts.
- g) Gifts and Traditional Hospitality which were deemed not culturally or religiously appropriate to reject have not been publically donated to charity publicizing the amount and source of funds, items or service.
- h) Not following Sucon's policies or procedures
- i) Fast-tracking or abusing the decision-making process.
- j) Unexplained preferences for certain sub-contractors.
- k) Invoices rendered or paid in excess of contractual amounts.

This list is not exhaustive and you should be alert to other indicators that may raise a suspicion of corrupt activity

9 REPORTING PROCESS AND PROCEDURES

Employees must report any suspected violations of this policy, or any incidents related to the misuse of Generative AI tooling, to the Sucon Council. All reports of suspected violations or incidents will be investigated promptly and thoroughly and as confidentially as possible. Employees must cooperate fully with any investigations related to suspected violations or incidents where Generative AI has been applied. Sucon prohibits retaliation against any employee who reports or participates in an investigation of a possible violation of our code of conduct, our policies including this policy, or the law. If you believe you are being retaliated against, please contact the Operations Manager or Vice President. Sucon reserves the right to review any communications sent through or information shared with Generative AI tooling to investigate suspected violations or incidents. This includes but is not limited to messages, prompts, attachments, and files.

9.1 Non-Compliance

Failure to comply with this Policy may result in severe consequences, which could include internal disciplinary action or termination of employment or consulting arrangements without notice in alignment with the Misconduct Process and Procedures' in the Human Resources

Once PRINTED, this is an UNCONTROLLED document. Please email info@sucon.ws for latest version.

Policy. Violation of this Policy may also constitute a criminal offence under Samoan, American Samoa, and New Zealand laws depending on where the project is stationed. If it appears in the opinion of the President's Council that any director, officer, employee, consultant or contractor of Sucon may have violated such laws, then Sucon may refer the matter to the appropriate regulatory authorities, which could lead to civil or criminal penalties for Sucon and/or the responsible person.

9.2 Appeal Process

Verdicts that are believed to be unfair by the Administration can be challenged via writing to the Council. Verdicts believed to be unfair by the Council must be challenged in writing to the Legal Counsellor as stipulated in the 'Misconduct Process and Procedures'

9.3 Whistle Blower Protection and Retaliation Prevention

It is the responsibility of all Sucon staff, Council, and affiliating members to protect the identity, security, and employment of the whistle-blower to prevent confrontation and retaliation from the alleged suspect and violator. Sucon staff, Council and affiliating members found to have leaked the identity of the whistle-blower are subject to suspension or termination by the Council or Administration depending on the level and severity of the case. Sucon staff, Council and affiliating members found to have participated directly or indirectly in retaliation are subject to suspension or termination by the Council or Administration depending on the level and severity of the case.

Whistle-blowers who are found to have falsified claims in an attempt for defamation are also subject to suspension or termination by the Council or Administration depending on the level and the severity of the case.

13. POLICY FEEDBACK

All Sucon employees and associates may provide feedback about this document by emailing info@sucon.ws

SUCON Consultancy Ltd

Telephone +0685 7519157

Address: Sucon Headquarters
Sanalele Complex, Vaea Street, Apia
Samoa

website <https://sucon.ws/>