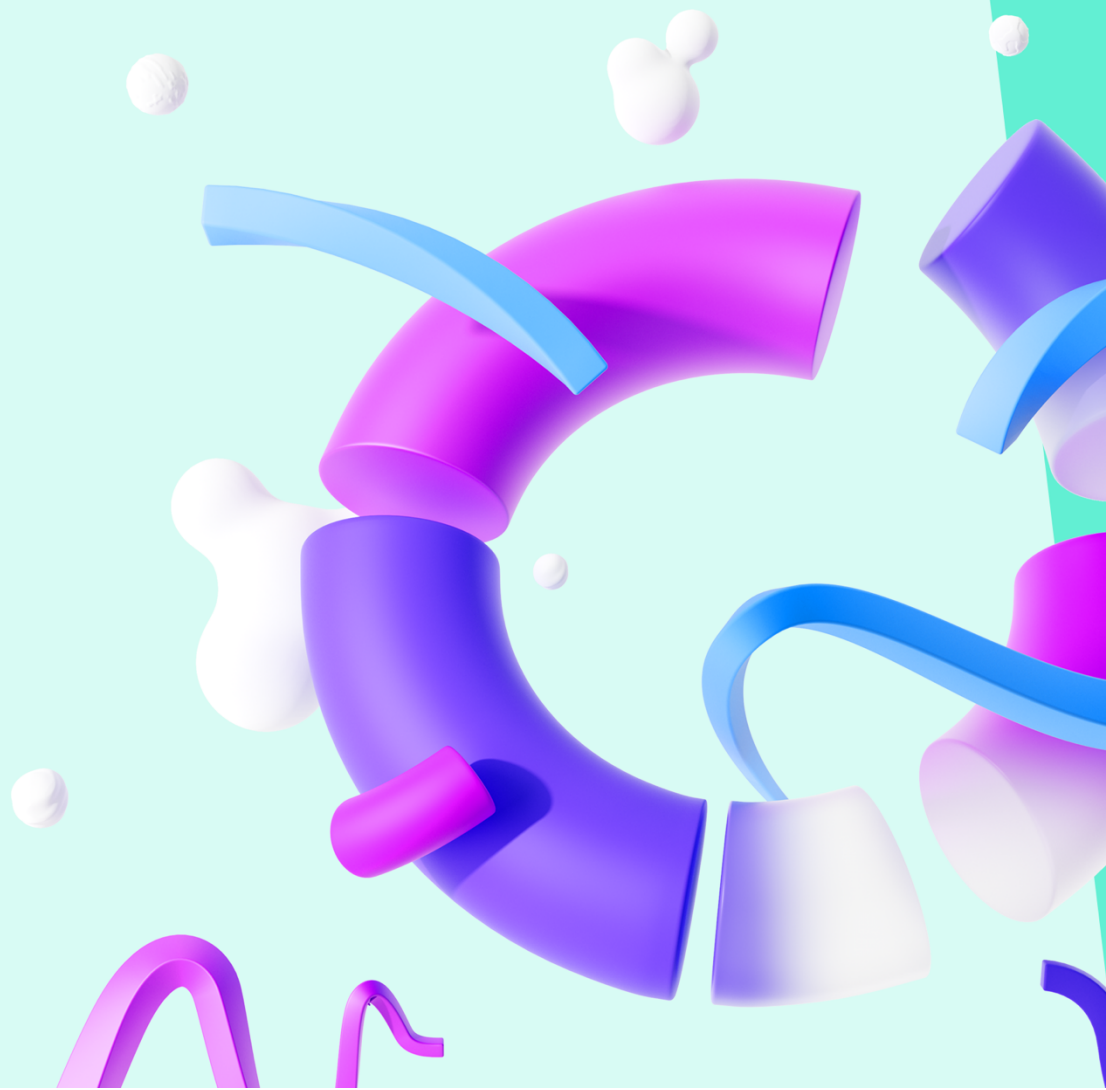


Walr

Information Security Policy Statement



Walr Information Security Policy Statement



Document Control

Owner:	ISMS Owner
Document Author:	Ollie Durrant
Issue Date:	17 th September 2024
Review Date:	17 th September 2025
Version:	V1.2
Description:	Walr Information Security Policy Statement
Security Classification	Public

Change History

Date	Version	Description of Modification	Modified By
11 th September 2024	0.1	Initial Draft	Ollie Durrant
12 th September 2024	1.0	Review and Approval	Simon Vaarning
13 th September 2024	1.1	Updated to include statement of commitment and commitment to improvement	Ollie Durrant
17 th September 2024	1.2	Updated company statement	Beth Hewitt

Walr Information Security Policy Statement



1 Purpose of Organisation

Walr is evolving the traditional online survey process with quantitative data creation infrastructure. It combines proprietary, unified technology, industry-leading audience reach, and best-in-class consultative expertise, to enable clients to make data-driven decisions at speed.

This policy's goal is to protect Walr against all internal, external, deliberate, and accidental threats which may cause a loss of confidentiality, integrity and availability to its information assets.

2 Information Security Statement

Information security is critical to the success and ongoing viability of Walr.

Our core security principle is to ensure the confidentiality, integrity and availability of the information we manage on behalf of our customers and business partners, as well as our own information.

As such, we aim to provide assurance to internal and external stakeholders, together with other interested parties, of the security and privacy of their information entrusted to Walr, whether in storage, processing or transmission.

To realise this principle, we are committed to the following security objectives:

- To protect our clients and their information;
- To ensure continued information security control during growth of our business;
- To enhance information security maturity within the Company;
- To continually identify, manage and treat information security risks;
- To report and investigate all known or suspected breaches of information security;
- To comply with the legal and regulatory frameworks under which our business operates; and
- To continually improve our information security management system.

This policy applies to:

- All full time, part time, temporary or casual Walr employees;
- All contractors engaged by Walr;
- All suppliers providing services to Walr; and
- Any other third parties with a valid reason to access Walr information.



3 Statement of Commitment

Due to the sensitive nature of information being stored, processed and transmitted, Walr is committed to ensure that information and information assets are properly safeguarded within a secure environment to protect their confidentiality, integrity and availability.

This Information Security Governance Framework provides a set of minimum information security requirements for managing risk to Walr information assets within the business. Walr develops and publishes procedures and processes to support compliance and operation of this framework. These artefacts establish objectives that can be used to assess the effectiveness of this framework.

Walr operates an ISMS that is compliant with the requirements of ISO 27001. All other supporting information security policies, standards, practices, procedures and guidelines provide the necessary detail to support the operations of the ISMS.

Compliance with the ISMS and its supporting policies, practices and procedures is mandatory.

4 Commitment to Continual Improvement

To ensure the continual improvement of the ISMS, regular steering committee meetings will be held.

Annual internal audits will take place to assess the company's compliance with the requirements of ISO 27001:2022 and the ISMS. Nonconformities will be reacted to and documented together with corrective actions.

Measures and metrics have been implemented to allow WALR to monitor and record progress against the objectives of the ISMS.

The SSC will undertake an annual management review of the operations of the ISMS. This review will assess the effectiveness, practicality and adequacy of the ISMS as a whole. Input from external and internal reviews, interested parties and audits will be considered during such reviews.

SV

Simon Vaarning, CTO

2024-09-17