KVQA Certification Services Private Limited

(https://www.kvqa.in)

ISO/IEC 27001:2022

CERTIFICATION AUDIT REPORT

WHILTER TECHNOLOGIES PRIVATE LIMITED

Document Control Information

Settings	
Document Title:	ISO/IEC 27001:2022 – Certification Audit Report
Project Title/Client Name:	**WHILTER TECHNOLOGIES PRIVATE LIMITED**
Document Authors:	Kush Kaushik
Doc. Version:	1.00
Sensitivity:	Confidential
Date:	24/05/2024

Disclaimer	Responsibility for the information and views set out in this document lies entirely with the authors. Reproduction is authorized provided the source is acknowledged.

TABLE OF CONTENTS

1 PURPOSE OF THE AUDIT 3

2 SCOPE OF THE AUDIT 3

3 RELATED DOCUMENTS 3

4 SAMPLING 4

5 SUMMARY OF AUDIT 5

6 CATEGORIZATION OF FINDINGS 6

7 AUDIT SUMMARY 7

7.1 Audit Information 7

7.2 Audit Report Distribution 7

7.3 Evaluation 7

7.3.1 Outcome of the Audit: 8

8 AUDIT RESULT 8

9 ISSUED CARS 9

10 DETAILED ACTION PLAN FOR NON-CONFORMANCE 10

11 OBSERVATION REPORT 11

1 PURPOSE OF THE AUDIT

The purpose of ISO/IEC 27001:2022 Certification Audit was to objectively evaluate adherence and the level of compliance to the requirements as these are defined in ISMS Documentation and the applicable standards ISO/IEC 27001:2022.

In addition, the audit aimed at examining any areas of potential improvement or inconsistencies in order to propose corrective or proactive/improvement actions.

2 SCOPE OF THE AUDIT

The ISO 27001:2022 Certification Audit was conducted for WHILTER TECHNOLOGIES PRIVATE LIMITED at following location & covered the following areas:

- Legislative Requirements and Compliance
- Semantics Requirements
- Organizational Requirements
- Operational Readiness
- Information Security
- Technical Requirements
- Networks

Location:

Location 1: 4TH FLOOR, UNIT NO 42, SUSHMA INFINIUM, NH 22 ZIRAKPUR, Mohali, SAS Nagar, Punjab, 140603

Location 2: B-18, Second Floor, Institutional Area, Sector 32, Gurugram, Haryana 122001

Scope:

The Information Security Management System (ISMS) at Whilter Technologies Private Limited applies to the AI/ML Services and SaaS platform - B2C communication for brands, reshaping ordinary text-based interactions into engaging personalized videos for their clients with the Support Function of IT Infrastructure, Human Resources, Physical Security, Legal and Administration.

This is in Accordance with Statement of Applicability Ver 1.0.

3 RELATED DOCUMENTS

[1] To reference here the applicable ISO 27001:2022 Audit Procedure (or Methodology)

[2] Reference of the Checklist for Information Security

[3] Below Client Documentation during Stage 1 Audit evidenced. –

S.No.	Document Name	Version	Release/Review Date	Description
1	Annexure A- Internal and External Issues	V1.0	01st Mar, 2024	Initial Release
2	Annexure B- Needs Expectations of interested parties	V1.0	01st Mar, 2024	Initial Release
3	Annexure C- Scope Statement	V1.0	01st Mar, 2024	Initial Release
4	Annexure D- CFT(ISG)_ Roles _Responsibilities	V1.0	01st Mar, 2024	Initial Release
5	Annexure G- Communication matrix	V1.0	01st Mar, 2024	Initial Release
6	Annexure H- Monitoring _ Measurement matrix	V1.0	01st Mar, 2024	Initial Release
7	Acceptable Usage Policy	V1.0	01st Mar, 2024	Initial Release

8	Antivirus Policy	V1.0	01st Mar, 2024	Initial Release
9	Asset Management Policy _ Procedure	V1.0	01st Mar, 2024	Initial Release
10	Background Check Policy	V1.0	01st Mar, 2024	Initial Release
11	BCP_DR Policy and Procedure	V1.0	01st Mar, 2024	Initial Release
12	BYOD Policy	V1.0	01st Mar, 2024	Initial Release
13	Change Management Policy _ Procedure	V1.0	01st Mar, 2024	Initial Release
14	Clear Desk _ Screen Policy	V1.0	01st Mar, 2024	Initial Release
15	Communication Procedure	V1.0	01st Mar, 2024	Initial Release
16	Correction and Corrective Action Procedure	V1.0	01st Mar, 2024	Initial Release
17	Cryptography Policy and Procedure.docx	V1.0	01st Mar, 2024	Initial Release
18	Data and Record Retention Policy.docx	V1.0	01st Mar, 2024	Initial Release
19	Data Backup Policy	V1.0	01st Mar, 2024	Initial Release
20	Data Privacy Policy	V1.0	01st Mar, 2024	Initial Release
21	Document Control Procedure	V1.0	01st Mar, 2024	Initial Release
22	External Provider Management Policy _ Procedure	V1.0	01st Mar, 2024	Initial Release
23	Form_Security Incident Final Report	V1.0	01st Mar, 2024	Initial Release
24	Hardening Policy	V1.0	01st Mar, 2024	Initial Release
25	HR Disciplinary Action Policy _ Procedure	V1.0	01st Mar, 2024	Initial Release
26	HR Security Policy	V1.0	01st Mar, 2024	Initial Release
27	IA Procedure	V1.0	01st Mar, 2024	Initial Release
28	Incident Management Policy and Procedure	V1.0	01st Mar, 2024	Initial Release
29	Information Classification Policy	V1.0	01st Mar, 2024	Initial Release
30	Information Security Policy	V1.0	01st Mar, 2024	Initial Release
31	IS Acquisition, Development and Maintenance Policy	V1.0	01st Mar, 2024	Initial Release
32	ISMS Manual	V1.0	01st Mar, 2024	Initial Release
33	ISMS Roles and Responsibilities	V1.0	01st Mar, 2024	Initial Release
34	Key Management Policy	V1.0	01st Mar, 2024	Initial Release
35	Legal _ Regulatory Compliance Register	V1.0	01st Mar, 2024	Initial Release
36	List of Internal Auditors	V1.0	01st Mar, 2024	Initial Release
37	Log Management and Monitoring Policy and Procedure	V1.0	01st Mar, 2024	Initial Release
38	Logical Access Control Policy _ Procedure	V1.0	01st Mar, 2024	Initial Release
39	Management Review Meeting Procedure	V1.0	01st Mar, 2024	Initial Release
40	Media Handling and Disposal Policy	V1.0	01st Mar, 2024	Initial Release
41	Mobile Device Policy	V1.0	01st Mar, 2024	Initial Release
42	Network Management Policy	V1.0	01st Mar, 2024	Initial Release
43	Password Management Policy	V1.0	01st Mar, 2024	Initial Release
44	Patch_Vulnerability Management Policy	V1.0	01st Mar, 2024	Initial Release
45	Physical _ Environmental Security Policy	V1.0	01st Mar, 2024	Initial Release
46	Physical Access Control Policy	V1.0	01st Mar, 2024	Initial Release
47	Risk Assessment Procedure	V1.0	01st Mar, 2024	Initial Release
48	Risk Register	V1.0	01st Mar, 2024	Initial Release
49	SDLC Policy	V1.0	01st Mar, 2024	Initial Release
50	Software Installation Policy _ Procedure	V1.0	01st Mar, 2024	Initial Release
51	Configuration Management Procedure and Policy	V1.0	01st Mar, 2024	Initial Release
52	Data Deletion Policy - v1	V1.0	01st Mar, 2024	Initial Release
53	Information Security Management System Manual	V1.0	01st Mar, 2024	Initial Release
54	Statement of Applicability (SoA) _ ISO 27001_2022	V1.0	01st Mar, 2024	Initial Release
55	Threat Intelligence Policy - template	V1.0	01st Mar, 2024	Initial Release

4 SAMPLING

The samples selected are all part of Organization's environment in scope. It was noted that most of the systems were configured with redundancy feature for high availability. The assessor sampled each asset from each system and sampled all single instances if multiple assets were not configured. All the servers/production instances are configured and hardened as per industry best practices. The assessor has sampled at least one sample from each category. The network is also configured as per standard network hardening guidelines. This way the assessment covered the entire scope of systems. The assessor also verified that each system from total population is reviewed as part of the sampling mechanism. All single instances of the environment were selected.

The sampling selected, covers all the system components and processes, including but not limited to Networks, Applications, Databases, Servers, Information Systems, and other supporting functions within organization.

5 SUMMARY OF AUDIT

This Certification Audit of ISMS was conducted on 24th May, 2024 by Lead Auditor Mr. Kush Kaushik to verify the onsite implementation as per requirements of the standard ISO27001:2022 respectively. The objective of this audit is the determination of conformity with audit criteria and the evaluation of the ability and effectiveness of the implemented management system as per requirements of ISO 27001:2022. ISMS Manual, policies and procedures were evidenced which meets the requirements of the standards. Internal and external issues are described as documented. The organization has trained and qualified personnel.

The organisation production environment is hosted on AWS. The Business Continuity and Service Continuity testing plan in place and testing happens on periodic basis.

ISMS Policy, Objectives and process flow chart are documented. External issues identified are with the context of Human Resources, Information Technology, IT equipment and support equipment. Internal issues identified are Suppliers, Employees, Customers, and Subcontractors.

The organization has a documented Risk Assessment Procedure, which contains the methodology of Risk Assessment and a documented Risk Register. The risk register contains risks related to ISMS and Project Specific along with its mitigation plan & risk owners.

The main goal of this exercise consists of a baseline assessment of the current basic and core system controls at WHILTER TECHNOLOGIES PRIVATE LIMITED. This assessment covered all relevant information, reflecting planned production site assessment activities and requirements.

Our review involved focus on processing, handling, transmission, and storage of data. Our main elements of the security assessment were People, Process and Technology.

Controls of ISO 27002	Count	% of Total Count
Minor Non-Conformance	0	0
Controls Compliant	93	100
Total Count	**93**	**100%**

The organization is recommended for Certification of ISO/IEC 27001:2022.

6 CATEGORIZATION OF FINDINGS

For the purpose of the audit, the definitions that will be used to classify the findings are detailed in the Audit Framework:

Findings Category	Type	Severity Description	Follow-up Timeframe	Closure Timeframe
Major-Non-Conformance	Major	Based on objective evidence, the absence of, or a significant failure to implement and/or maintain conformance to the requirements of the applicable standard. (i.e. the absence of or failure to implement a complete Management Systemclause of the standard); or A situation which would on the basis of available objective evidence, raise significant doubt as to the capability of the Management System to achieve the stated policy and objectives of the customer.	Re-Audit	N/A
Minor Non-Conformance	Minor	Represents either a management system weakness or minor issue that could lead to a major nonconformance if not addressed. Each minor NC should be considered for potential improvement and to further investigate any system weaknesses for possible inclusion in the corrective action program.	Within 1 Month	Within1 Month
Observation	Point of Improvement	The Good Points observed during the Audit and also potential points of improvement.	N/A	N/A

7 AUDIT SUMMARY

7.1 Audit Information

Audit Date: 24th May, 2024

Audited Entity: WHILTER TECHNOLOGIES PRIVATE LIMITED.

Auditees: Sunil Bansal, Pankaj Arora, Krishna Tiwari

Auditor(s): Jayshree Dutta

7.2 Audit Report Distribution

KVQA Assessment Committee

Head – WHILTER TECHNOLOGIES PRIVATE LIMITED

Head of Steering Committee WHILTER TECHNOLOGIES PRIVATE LIMITED

7.3 Evaluation:

Overall evaluation of audit review

(Effectiveness of the system, Requirements for Improvement)

The management commitment in the form of ISMS policy and Objectives were found to be documented. The incident handling procedure found, and all incidents logged with Corrective Action/PA done. Statement of Applicability found appropriate. The Organization has a documented Risk and Opportunity Management Register. As per which the risk assessment has been done and documented into Risk Register.

The Organization has documented all policies and procedures as per the requirement of the standard. The Company has trained and qualified Personnel. Detailed Internal Audits and MRMs are being conducted.

Strengths –

- The Organization has developed ISMS Objectives and it is being tracked on periodic basis.
- Detailed description of External and Internal Issues evident
- The organization has documented Risk Assessment criteria according to which Risk Assessment is conducted.
- The organization has a detailed Non-Disclosure Agreement signed by their permanent employees.
- All new employees had undergone training including security trainings.
- Access review is being done during the audit period.
- Incident management has been implemented.

This ISMS Certification assessment of WHILTER TECHNOLOGIES PRIVATE LIMITED evaluated the implementation of all 93 Control Status and Management System Control Status of the requirements in the ISO 27001:2022 standard and the organization have shown to achieve the objectives of the standard within its following key areas.

- Access Control.
- Security Policy.
- Organization of Information Security.
- Asset Management.

- Human Resources Security.
- Cryptography.
- Communications, Supplier and Operations Management.
- Information Systems Acquisition, Development and Maintenance.
- Information Security Incident Management
- Business Continuity Management; and
- Compliance

The details of observation are annexed in Observation report. No Major or Minor Non-Conformance was observed. The auditors are convinced that after implementation of the Point of Improvement, the company will have a better Information Security Management System at **WHILTER TECHNOLOGIES PRIVATE LIMITED.** The observation compliance for corrective action shall be verified in the next audit; hence the company is recommended for the certificate.

7.3.1 Outcome of the Audit:

✔ Successfully passed the audit.
Your system is practiced without any serious major non-conformances. Non-Conformance closure evidence to be submitted within 30 days. Observations shall be verified in the next Surveillance Audit.
☐ After on-site visit as follow-up, this will be resolved
No Non-conformity is found in your system as shown from above CAR issues. You are required to submit the result of corrective action taken, which includes corrective action, analysis of the reason, and preventive action to KVQA within 1 month.
☐ Not to satisfy with standard
Major non-conformities are found in your system as shown from above CAR issues.
Re-audit is required □Yes ☑No
Fees Remitted or not? ☑Yes □No (When audit fee is paid, Surveillance will be issued

8 AUDIT RESULT

☑Recommend Certification /Continuation of Certification

The system is proper and effectively practiced, ISO 27001:2022 Certification is recommended.

9 NON-CONFORMANCE & OBSERVATION REPORT

The below points are observations from the Audit which includes potential points of improvements and good points observed.

Sr. No.	Nature of Findings	Department	Standard reference	Description
1	Good Observation	IT Operations	ISO 27001:2022	Asset Inventory was updated and asset tags has been provided to all the assets.
2	Good Observation	Governance	ISO 27001:2022	BCP test has been performed as per requirements.
5	Good Observation	Human Resources	ISO 27001:2022	Signed NDA could be evidenced for employees during the Audit
6	Good Observation	Human Resources	ISO 27001:2022	Manpower planning process is well documented and tracked
7	Good Observation	Human Resources	ISO 27001:2022	Performance review process is well documented and implemented
8	Good Observation	IT Networks	ISO 27001:2022	Windows Defender Endpoint solution is running as Antivirus on all the systems
9	Good Observation	Governance	ISO 27001:2022	The Company has defined the limits and applicability of its ISMS in order to define its scope.
10	Good Observation	Governance	ISO 27001:2022	Risk Assessment with mitigation plan are updated and maintain
11	Good Observation	Operations	ISO 27001:2022	Objectives for organisation were defined and progress is been monitored.

……END OF REPORT……