## 0.1 Approval and Issue

This document is the property of VISTA InfoSec and shall not be reproduced in part or in full without its written consent.

**Reviewed by :** **Management Representative**

**Approved by :** **Chief Executive Officer**

**Note:**

1. The Management Representative is responsible for the issue and distribution of this document, including amendments.
2. The holder of this copy is responsible for incorporating all amendments and for ensuring the currency of the document.

## 0.2 Amendment Record

| Amendment No. | Date of Amendment | Nature of Amendment | Page Ref. |
|---|---|---|---|
| Issue 1.0 / Rev 1.0 | 26.08.2026 | First issue. Certification agreement established exclusively for ISMS certification in accordance with ISO/IEC 27001:2022 including Amendment 1:2024 (Climate action changes), ISO/IEC 17021-1:2015 and ISO/IEC 27006-1:2024. | All |
| | | | |
| | | | |
| | | | |
| | | | |

## 1.0 Purpose and Scope

1.1 The purpose of this document is to define the legally enforceable agreement between VISTA InfoSec (the Certification Body) and its clients for the certification of Information Security Management Systems (ISMS) against ISO/IEC 27001:2022, including Amendment 1:2024, and to ensure that clients abide by the rules and requirements of the VISTA InfoSec ISMS certification scheme.

1.2 This document covers the terms and conditions of certification, including the mutual rights and obligations of the client and the Certification Body, the right to use the certificate and certification mark, and the coverage of all sites within the scope of certification.

## 2.0 Responsibility

| Role | Responsibility |
|---|---|
| Operations / Certification Team | Ensure that the agreement is signed by the client without any dissent before the start of the initial (Stage 1) audit, and that the signed original is retained in the client file. |
| Client | Abide by the terms and conditions laid down in this agreement and the certification requirements of the Certification Body. |
| Certification Body (VISTA InfoSec) | Provide ISMS audit and certification services to the client impartially and competently, in accordance with this agreement. |

## 3.0 Associated and Reference Documents

**Associated documents (VISTA InfoSec)**

1. VI/AM/AA-01 VISTA APEX Manual
2. VI/PM-ISMS/AA-02 ISMS Scheme Manual
3. VI/PM/AA-06 Procedure for Use of Certificate and Certification Mark
4. VI/PM-ISMS/AA-03 ISMS Procedure Manual
5. VI/PM//AA-12 Procedure for handling Appeals
6. VI/PM/AA-15 Procedure for handling Complaints
7. VI/AIMS_ISMS/FF-16 Schedule of Certification Fees

**Reference standards and mandatory documents**

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27001:2022/Amd 1:2024 Climate action changes
- ISO/IEC 27002:2022 Information security controls
- ISO/IEC 27000 Information security management systems — Overview and vocabulary
- ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements
- ISO/IEC 27006-1:2024 Requirements for bodies providing audit and certification of information security management systems — Part 1: General
- IAF Mandatory Documents as applicable, including IAF MD 1 (multi-site), IAF MD 2 (transfer of certification), IAF MD 4 (use of ICT for auditing), IAF MD 5 (audit time) and IAF MD 11 (integrated audits)
- Requirements of the accreditation body, as applicable

## 4.0 Definitions

For the purpose of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 17021-1 and the VISTA InfoSec ISMS Certification Manual apply. Additional definitions specific to the agreement are given in Article 2 of Annexure A.

## 5.0 Resources

The personnel resources for the activities described in this document are as identified in the VISTA InfoSec ISMS Certification Manual and the competence records of the Certification Body.

## 6.0 Procedure

6.1 Before proceeding with the audit, the Certification Body shall ensure that a legally enforceable agreement is in place with the client, which details the mutual rights and obligations of the client and the Certification Body, includes the right to use the certificate and certification mark, and, where the client has multiple sites, covers all sites within the scope of certification.

6.2 All responsibilities and obligations set out in this agreement shall be met by all concerned.

6.3 In pursuance of its policy of continual improvement, the Certification Body reserves the right to modify the content of its rules and procedures for ISMS certification, including changes arising from revisions or amendments of ISO/IEC 27001, ISO/IEC 27006-1 or accreditation requirements. Such changes shall be notified to clients well in advance, with reasonable time to prepare for any change in certification requirements.

6.4 The signed original of the certification agreement (VI/ISMS/FF-15) shall be retained in the client file by the CB operation Team. The content of the agreement shall be as given in Annexure A to this document.

## Part II : Annexure – A

# AGREEMENT FOR ISMS CERTIFICATION

**as per ISO/IEC 27001:2022 including Amendment 1:2024**

This Agreement is made on _____ between **VISTA InfoSec**, having its registered office at _____, hereinafter referred to as the **"Certification Body" (CB)**, and _____, having its principal office at _____ and the sites listed in Schedule 1 to this Agreement (attach additional sheets as needed), hereinafter referred to as the **"Client"**, which expression shall include its successors and permitted assigns.

## 1. INTRODUCTION

1.1 The CB provides audit and certification of Information Security Management Systems (ISMS) against ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, as amended by ISO/IEC 27001:2022/Amd 1:2024 (Climate action changes). The CB operates in accordance with ISO/IEC 17021-1:2015, ISO/IEC 27006-1:2024, the applicable IAF Mandatory Documents and the requirements of its accreditation body, _____ (where accredited).

1.2 This Agreement sets out the relationship between the CB and the Client, and the terms and conditions to be met by both parties in the operation of ISMS certification, including the right to use the certificate and certification mark.

1.3 The Client's application form, the CB's proposal / quotation, Schedule 1 (Scope and Sites) and the CB's rules for the use of the certificate and certification mark form part of this Agreement.

1.4 Both the CB and the Client shall abide by the letter, spirit and intent of this Agreement.

## 2. DEFINITIONS

2.1 **ISMS** means the Client's information security management system as defined in ISO/IEC 27000 and established in accordance with ISO/IEC 27001:2022 including Amd 1:2024.

2.2 **Scope of certification** means the boundaries and applicability of the ISMS certified by the CB, including the organizational units, processes, locations, information assets and technologies covered, as stated on the certificate.

2.3 **Statement of Applicability (SoA)** means the documented statement required by clause 6.1.3 d) of ISO/IEC 27001:2022 describing the necessary controls, the justification for their inclusion and exclusion, and their implementation status.

2.4 **Certification documents** means the certificate, its annexures and schedules, and the audit reports issued by the CB.

2.5 **Special audit** means an audit, other than a planned surveillance or recertification audit, conducted for extension of scope or at short notice in accordance with Article 3.8.

## 3. CERTIFICATION PROCESS

3.1 The Client shall provide accurate and complete information at the time of application and whenever requested, including the intended scope, sites, total and effective number of personnel, shifts, outsourced processes and suppliers relevant to the ISMS, legal, regulatory and contractual requirements, the current version of the SoA, the use of any consultancy relating to the ISMS, and any existing certifications. The CB will conduct an application review and determine audit time in

accordance with ISO/IEC 27006-1 and IAF MD 5, and, for multi-site organizations, apply sampling only where, permitted by ISO/IEC 27006-1 and IAF MD 1.

3.2 The initial certification audit shall be conducted in two stages:

(a) **Stage 1** — review of the Client's documented ISMS information, including the ISMS scope; context of the organization, including the determination of whether climate change is a relevant issue (clause 4.1); the needs and expectations of interested parties, including any climate-related requirements (clause 4.2); the information security policy and objectives; the risk assessment and risk treatment process and results; the SoA; and evidence of internal audit and management review, in order to determine readiness for Stage 2.

(b) **Stage 2** — evaluation of the implementation and effectiveness of the ISMS, including the controls declared in the SoA, at the Client's site(s).

3.3 Before the Stage 2 audit, the Client's ISMS shall be operational, and at least one internal audit and one management review covering the scope of certification shall have been completed.

3.4 Nonconformities identified during any audit shall be addressed by the Client through correction, root cause analysis and corrective action within the timeframe specified by the CB. Certification will not be granted until all major nonconformities have been closed and the CB has reviewed and accepted the plans for minor nonconformities. If the CB is unable to verify the implementation of corrections and corrective actions for any major nonconformity within six (6) months after the last day of Stage 2, the CB shall conduct another Stage 2 audit before recommending certification.

3.5 The certification decision shall be taken by competent person(s) of the CB who were not involved in the audit. Where certification is granted, the CB will issue a certificate valid for three (3) years, subject to successful surveillance. The certificate will state the scope of certification, the certified site(s), the standard (ISO/IEC 27001:2022, with reference to Amd 1:2024 as required by the CB and accreditation body) and a reference to the specific version of the SoA.

3.6 Surveillance audits shall be conducted at least once each calendar year, except in recertification years. The date of the first surveillance audit following initial certification shall not be more than twelve (12) months from the date of the certification decision. Surveillance will include, among other things, internal audits and management review, actions on nonconformities, complaints, changes to the ISMS and SoA, the effectiveness of the ISMS in achieving its objectives, and the continuing consideration of climate change and other context issues.

3.7 A recertification audit shall be planned and conducted before the expiry of the certificate. The Client shall apply for recertification sufficiently in advance. If recertification activities are not completed, or the certification decision is not taken, before the expiry date, certification shall lapse. Certification may be restored within six (6) months of expiry provided outstanding recertification activities are completed; otherwise, at least a Stage 2 audit shall be conducted.

3.8 The CB may conduct special audits for extension of scope, and short-notice or unannounced audits to investigate complaints, respond to changes notified by the Client, follow up on suspended certification, or as otherwise reasonably required. The Client shall not unreasonably refuse such audits.

3.9 The CB will inform the Client in advance of the audit plan and the names of the audit team members, including any technical experts and observers. The Client may object to the appointment of any audit team member with documented justification (for example, a conflict of interest), and the CB will review such objection.

3.10 Where agreed by both parties and permitted by the CB's risk assessment, audit activities may be conducted remotely using information and communication technology (ICT) in accordance with IAF MD 4. The Client shall provide the secure means and access needed for this. Audio or video recording of audit sessions shall be made only with the mutual consent of both parties.

3.11 Transfer of certification from another accredited certification body, and integrated audits with other management system standards, shall be carried out in accordance with IAF MD 2 and IAF MD 11 respectively, where applicable.

## 4. OBLIGATIONS OF THE CLIENT

4.1 The Client shall at all times comply with the requirements of ISO/IEC 27001:2022 including Amd 1:2024, the certification requirements of the CB and the terms of this Agreement and shall maintain its ISMS effectively throughout the period of certification. In particular, the Client shall:

(a) determine whether climate change is a relevant issue for its ISMS, and consider climate-related requirements of relevant interested parties, addressing them within the ISMS where relevant;

(b) maintain its information security risk assessment, risk treatment plan and SoA, and review them when significant changes occur;

(c) conduct internal audits and management reviews at planned intervals and act on their results;

(d) maintain documented information as required by ISO/IEC 27001:2022 and make it available to the CB.

4.2 The Client shall make all necessary arrangements for the conduct of audits, including provision for examining documentation and records, and access to relevant equipment, locations, areas, personnel, information systems (where appropriate) and the Client's subcontractors and outsourced processes within the scope of certification.

4.3 Where any ISMS-related information or record cannot be made available to the audit team because it contains confidential or sensitive information, the Client shall inform the CB in advance (at application or before Stage 1). The CB will determine whether the ISMS can be adequately audited in the absence of such information; if it cannot, the audit may not proceed until appropriate access arrangements are agreed.

4.4 The Client shall, when requested by the CB, allow access to observers, including assessors of the accreditation body witnessing the CB's audit, trainee auditors and other observers agreed in advance, and shall allow access to the accreditation body for independent or validation visits.

4.5 The Client shall:

(a) only claim that it is certified with respect to the scope for which certification has been granted;

(b) use the certificate and certification mark of the CB, and any accreditation mark, only in accordance with the CB's rules for use of the certificate and mark, and not on products, product packaging, or laboratory test, calibration or inspection reports or certificates, or in any way that implies that a product, process or service is certified;

(c) not use its certification in a manner that brings the CB or the certification into disrepute, and not make any statement regarding its certification that the CB may consider misleading or unauthorized; and take immediate corrective steps where the CB so requires;

(d) make it clear in its contracts, publicity and guidance documents that ISMS certification does not imply that any product, service or process is certified or approved by the CB;

(e) upon suspension or withdrawal of certification, discontinue its use of all advertising matter that contains any reference to certification, and return or destroy the certificate as directed by the CB; upon reduction of scope, amend all advertising matter accordingly;

(f) when providing copies of certification documents to others, reproduce them in their entirety or as specified by the CB;

(g) keep a record of all complaints made known to it relating to compliance with ISMS requirements, take appropriate action, document the actions taken, and make these records available to the CB on request;

(h) make available to the CB, on request or during audits, records of complaints, appeals and disputes relating to its certification;

(i) pay all fees and charges due to the CB promptly, in accordance with Article 11.

4.6 The Client shall inform the CB, without delay and wherever practicable before implementation, of changes that may affect the capability of the ISMS to continue to fulfil the requirements of the standard used for certification, including changes in:

(a) legal, commercial or organizational status or ownership;

(b) organization and management, including top management and key managerial or decision-making personnel;

(c) contact address and sites, including addition, closure or relocation of sites;

(d) the scope of operations under the certified ISMS, including significant changes in the number of personnel, information processing facilities, technologies or outsourced processes;

(e) major changes to the ISMS, its processes, risk assessment or the SoA;

(f) any significant security incident or breach, and any regulatory action or legal proceedings, relevant to the certified ISMS.

4.7 The CB may, upon notification of such changes, conduct a special audit, review the scope of certification or take other action as appropriate.

4.8 The Client shall not offer any gift, payment or other inducement to CB personnel and shall disclose to the CB any relationship that may affect the impartiality of the audit team.

## 5. OBLIGATIONS OF THE CERTIFICATION BODY

5.1 The CB shall carry out its certification activities impartially, consistently and in a non-discriminatory manner, using auditors and technical experts whose competence meets the requirements of ISO/IEC 17021-1 and ISO/IEC 27006-1.

5.2 The CB shall not offer or provide ISMS consultancy, or internal information security audits, to the Client, and shall not certify the Client's ISMS where any of its personnel or a related body has provided ISMS consultancy to the Client within the previous two (2) years.

5.3 The CB shall provide the Client with a detailed description of the certification activities, the requirements for certification, information about fees, the audit plan, the audit report and the outcome of the certification decision.

5.4 The CB shall give the Client due notice of any changes to its certification requirements, including those resulting from revisions or amendments to ISO/IEC 27001 or accreditation requirements, and allow reasonable time for the Client to implement them. The Client shall notify the CB of the completion of such changes within the time allowed, and the CB will verify their implementation.

5.5 The CB shall maintain and make publicly available, or provide on request, information on the status of certification (valid, suspended or withdrawn), the name of the Client, the scope, sites and standard of certification, and may upload such information to the IAF CertSearch database or any database required by its accreditation body.

## 6. SUSPENSION, WITHDRAWAL AND REDUCTION OF SCOPE

6.1 The CB may suspend certification where, among other things:

(a) the Client's ISMS has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the ISMS;

(b) the Client does not allow surveillance or recertification audits to be conducted at the required frequency;

(c) the Client has voluntarily requested a suspension;

(d) the Client misuses the certificate or certification mark, or fails to pay fees due;

(e) the Client fails to comply with any other term of this Agreement.

6.2 During suspension, the Client's certification is temporarily invalid and the Client shall refrain from further promotion of its certification. The period of suspension shall not normally exceed six (6) months. Failure to resolve the issues that led to suspension within the time set by the CB shall result in withdrawal of certification or reduction of scope.

6.3 The CB shall reduce the scope of certification to exclude the parts not meeting the requirements where the Client has persistently or seriously failed to meet the certification requirements for those parts of the scope.

6.4 Additionally, the CB reserves the right to withdraw certification if the Client:

(a) enters into liquidation, whether compulsory or voluntary (other than for the purposes of reconstruction or amalgamation), or has a receiver or administrator appointed for its business;

(b) fails in any respect to comply with the law of the land relevant to the certified ISMS;

(c) fails to comply with the conditions specified in the CB's certification procedures.

6.5 Upon suspension or withdrawal of certification, however determined, the Client shall forthwith discontinue its use of any reference to certification. The CB will publish information on suspension, withdrawal or reduction of scope in its directory of certified clients.

## 7. CONFIDENTIALITY AND DATA PROTECTION

7.1 All information obtained or created by the CB, its auditors, technical experts and staff during the performance of certification activities, other than information already in the public domain or which the Client makes publicly available, shall be treated as confidential and shall not be disclosed without the prior written consent of the Client, except as required by law or by the accreditation body.

7.2 Where the CB is required by law or authorized by contractual arrangements to release confidential information, the Client shall be notified of the information provided, unless prohibited by law. Information about the Client obtained from sources other than the Client (for example, a complainant or regulator) shall also be treated as confidential.

7.3 The Client agrees that the information listed in Article 5.5 may be made publicly available, and that the accreditation body may access the CB's records relating to the Client under conditions of confidentiality.

7.4 The CB shall protect information obtained from the Client in accordance with the CB's own information security controls. Auditors shall not remove copies of the Client's confidential documents or records from the Client's premises unless agreed with the Client, and audit evidence shall be limited to what is necessary to support audit findings.

7.5 Personal data exchanged under this Agreement shall be processed by each party in accordance with applicable data protection laws, including the Digital Personal Data Protection Act, 2023 (India), and only for the purposes of this Agreement.

## 8. CERTIFICATE AND USE OF THE CERTIFICATION MARK

8.1 The certificate and the certification mark remain the property of the CB. The Client acknowledges receipt of the CB's rules for the use of the certificate and certification mark, and of any applicable accreditation body rules, and agrees to comply with them.

8.2 The Client may use in its documents, brochures or advertising media, without variation, the phrase: "ISMS certified to ISO/IEC 27001:2022 by VISTA InfoSec for the scope: _____ (Certificate No. _____)".

## 9. APPEALS

9.1 The Client may appeal against any certification decision of the CB, including a decision to refuse, suspend, withdraw or reduce certification, or to refuse an extension of scope. Such a decision shall stand pending the outcome of the appeal.

9.2 Appeals shall be made in writing within thirty (30) days of communication of the decision and will be processed in accordance with the CB's Appeals Procedure, which is publicly available or provided on request. The appeal will be reviewed by person(s) not involved in the decision under appeal, and the outcome communicated in writing.

## 10. COMPLAINTS

10.1 Complaints regarding the CB, its audit teams or its certification activities shall be addressed in writing to the Head – Certification, VISTA InfoSec.

10.2 Complaints will be acknowledged, investigated and resolved in accordance with the CB's Complaints Procedure, which is publicly available or provided on request. Where the complainant is not satisfied with the outcome, the complaint may be referred to the accreditation body.

## 11. FEES

11.1 The Client shall pay the CB's fees for application, audit, certification, surveillance, recertification and special audits as stated in the CB's proposal / quotation, together with applicable taxes and reasonable travel and accommodation expenses, within the payment terms stated therein.

11.2 Cancellation or postponement of a confirmed audit by the Client at short notice may attract charges as stated in the proposal. The CB's fees are subject to periodic revision; the Client will be informed of any revision well in advance and provided with a revised quotation for continuation of certification.

## 12. ASSIGNMENT

Except as otherwise agreed by the parties in writing, neither this Agreement nor the certification granted under it shall be assigned or transferred.

## 13. LIABILITY

13.1 No representation, promise or warranty, express or implied, is or will be made or given as to the accuracy or completeness of any information, review or audit supplied, made or given by the CB (or any of its directors, employees, auditors or technical experts) in the course of providing services pursuant to this Agreement, and no such person is authorized to make or give any such representation, promise or warranty. Any representation, promise or warranty purported to be so made or given shall not be relied upon.

13.2 Certification does not alter the contractual responsibilities between the Client and its customers. While ISMS certification is an indication of the Client's capability to manage information security in line with ISO/IEC 27001:2022, it does not constitute a guarantee by the CB that the Client will maintain a

particular level of performance or that information security incidents will not occur. The CB shall not be liable for any deficiency in the products or services supplied by the Client.

## 14. FORCE MAJEURE

No failure or omission by either party to carry out or observe any of the stipulations, conditions or warranties of this Agreement shall give rise to any claim against such party, or be deemed to be a breach of contract, to the extent that such failure or omission arises from causes reasonably beyond the control of such party. In such extraordinary events, the CB may apply the relevant IAF and accreditation body guidance, including the use of remote audit techniques or the rescheduling of audits.

## 15. INDEMNITY

The Client undertakes to indemnify the CB against any losses suffered by, or claims made against, the CB as a result of the misuse by the Client of its certification status, certificate or certification mark, or as a result of any breach by the Client of the terms of this Agreement.

## 16. GOVERNING LAW AND JURISDICTION

This Agreement shall in all respects be construed and operate as an agreement made in India and shall be governed by the laws of India, subject to the exclusive jurisdiction of the courts at _____.

## 17. ARBITRATION

All disputes, differences or questions arising between the parties as to the construction of this Agreement, or any matter arising out of or in connection with it, which cannot be settled by mutual agreement, shall be referred to a sole arbitrator appointed by mutual consent of the parties. The arbitration shall be conducted in accordance with the Arbitration and Conciliation Act, 1996, the seat of arbitration shall be ____Mumbai_____, and the language of arbitration shall be English.

## 18. TERMINATION

18.1 This Agreement shall continue in force unless and until terminated:

(a) by either party upon ninety (90) days' written notice to the other; or

(b) immediately by decision of the CB upon withdrawal of certification, in accordance with the CB's procedures and as formally notified to the Client.

18.2 A Client wishing to relinquish its certification shall give written notice to the CB of its intent, stating the arrangements made for settlement of any outstanding fees.

18.3 Upon termination, whether by notice, default or otherwise, the certificate issued under this Agreement shall become invalid from the date of termination, and the Client shall immediately cease to use it and the certification mark and return or destroy all certification documents as directed by the CB. The Client shall remain bound by the provisions of this Agreement that by their nature survive termination, including Articles 7, 13 and 15.

## 19. NOTICES

Any notice or communication under this Agreement shall be in writing and shall be deemed duly given if sent by registered / speed post, courier or e-mail to the address or e-mail address of the other party last notified in writing, and shall be deemed received at the time it would have been delivered in the ordinary course of post or, for e-mail, upon successful transmission.

## 20. ENTIRE AGREEMENT AND AMENDMENT

This Agreement, together with the documents referred to in Article 1.3, constitutes the entire agreement between the parties in respect of ISMS certification. The Client will be given due notice of any proposed changes to this Agreement, and reasonable time to make any necessary adjustments.

## 21. THE PARTIES TO THE AGREEMENT

| For the Client | For the Certification Body |
|---|---|
| Name of Organization: | Name of Organization: VISTA InfoSec Pvt Ltd., |
| Address: | Address: |
| Name of Authorized Signatory: | Name of Authorized Signatory: |
| Designation: | Designation: |
| Signature & Seal: | Signature & Seal: |
| Date: | Date: |

## Schedule 1 – Scope of Certification and Sites

**Proposed scope of certification:**

| |
|---|
| |

**Statement of Applicability reference (version and date): _____**

**Sites covered by the scope of certification:**

| Sl. No. | Site Name | Address | No. of Personnel | Activities / Processes |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |

*(Attach additional sheets if needed. Each sheet shall be signed by the authorized signatories of both parties.)*