Procedure for Managing Impartiality and confidentiality

DOCUMENT CONTROL

DOCUMENT NUMBER	*VI/PM/AA -11*	**ISSUE / REVISION**	1.0 / 1.0
DOCUMENT OWNER	Management Representative	**ISSUE DATE**	26 August 2026
PREPARED BY	VISTA InfoSec (CB)	**REVIEWED BY**	Management Representative
APPROVED BY	Chief Executive Officer	**NEXT REVIEW**	Twelve months from issue

CONFIDENTIAL

Property of VISTA InfoSec Private Limited. Not to be reproduced, copied, distributed or disclosed, in whole or in part, without prior written consent.

NOTE:

1. Management Representative is responsible for issue and distribution of this document including amendments.
2. Authorized user / Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

Contents

Statement of Impartiality: (Signed By CEO) 3
1. Purpose 3
2. Principle 4
3. Identification of Risks to Impartiality: 4
4. Risk Assessment Process 4
6. Monitoring and Continual Improvement 5
7. Record and Documentation 5
8. Conclusion 5

Contents and page numbers refresh automatically: select the list and press F9 in Word, or Tools ▸ Update ▸ Update All in LibreOffice.

Uncontrolled when printed, the approved version is held in the Certification Body document repository

Statement of Impartiality: (Signed By CEO)

M/s VISTA InfoSec as an CAB, recognizes the fundamental importance of impartiality, objectivity, and integrity in all its operations and decision-making processes.

We are fully committed to conducting all accreditation and approval activities in a fair, transparent, and non-discriminatory manner, ensuring that no undue influence, whether commercial, financial, or organizational, affects the outcome of any evaluation or accreditation decision.

TO UPHOLD THIS COMMITMENT:

1. M/s VISTA InfoSec has established a governance structure designed to safeguard impartiality, including independent oversight by the Impartiality Committee.
2. All personnel, secretariat, assessors, and committee members are required to act objectively and to disclose any potential conflicts of interest.
3. Policies, procedures, and operational controls have been implemented to identify, analyse, and mitigate risks to impartiality.
4. Access to accreditation and approval services is open to all eligible applicants, without discrimination based on size, ownership, affiliation, or membership in any association.
5. All decisions on accreditation or approval are based solely on objective evidence of competence and compliance with applicable standards.

M/s VISTA InfoSec. continually reviews and strengthens its impartiality framework to ensure alignment with ISO/IEC 17021-1:2015 and international best practices.
We affirm that impartiality is not only a policy but a core organizational value integral to our credibility, integrity, and public confidence in the digital conformity assessment ecosystem.

AUTHORIZED BY:

(Signature)
Name: ...Sd.....
Designation: CEO
Organization: M/s: VISTA InfoSec.

Date : .....
Document Reference :VI/PM/AA-11

Uncontrolled when printed, the approved version is held in the Certification Body document repository

Procedure: Risk to Impartiality – Identification and Mitigation Framework

This procedure clearly defines the process, accountability, and mechanisms to identify, analyze, and control risks to impartiality within the accreditation / approval operations of M/s VISTA InfoSec.

1. Purpose

The purpose of this framework is to ensure that M/s VISTA InfoSec systematically identifies, evaluates, and mitigates all potential risks to impartiality that may arise from its accreditation and approval activities

.This framework supports compliance with Clause 5.2 (Impartiality) of ISO/IEC 17021-1:2015 and reinforces stakeholder confidence in the independence, integrity, and credibility of accreditation decisions.

2. Principle

Impartiality is central to the integrity of all Certification operations. Any situation that could result in a conflict of interest, bias, or undue influence, whether actual, perceived, or potential—shall be identified and controlled through preventive and corrective mechanisms.

M/s VISTA InfoSec ensures that impartiality is maintained across all functions, from application to accreditation decision.

3. Identification of Risks to Impartiality:

Potential risks to impartiality may arise from, but are not limited to:

SR. NO.	CATEGORY	POSSIBLE SOURCE OF RISK	EXAMPLES
1.	**Organizational**	Structural or ownership links	Shared ownership, financial interests, or governance overlap between M/s VISTA InfoSec and CAB.
2.	**Personnel**	Individual conflict of interest	Assessors or decision-makers with prior consultancy, employment or or financial relationships with the applicant
3.	**Operational**	Involvement in other services	Participation in training, consultancy, or promotional activities that may influence assessment outcomes
4.	**Financial**	Revenue dependence	Excessive reliance on income from a specific client, sector, or activity influencing decision to impartiality
5.	**External Influence**	Political or commercial pressure	Interference from external bodies, regulators, or industry groups
6.	**Confidentiality Breach**	Improper disclosure of information	Sharing of confidential applicant data leading to perceived or real partiality

4. Risk Assessment Process

- ✓ **Identification** – Each function, activity, or relationship that could affect impartiality is reviewed and recorded in the Risk Register for Impartiality (Format VI/AIMS_ISMS/FF-35).
- ✓ **Analysis** – The probability of occurrence, potential impact and likelihood of each risk are assessed using qualitative criteria (Low, Medium, High).

Uncontrolled when printed, the approved version is held in the Certification Body document repository

- ✓ **Evaluation** – Risks are evaluated against acceptable thresholds defined in the Impartiality Risk Policy.
- ✓ **Mitigation / Control** – Appropriate control measures are implemented, such as:
  - Recusal of conflicted personnel.
  - External peer review or dual decision-making.
  - Separation of operational and decision-making roles.
  - Independent oversight by the Impartiality Committee.
- ✓ **Monitoring and Review** – Risks and controls are reviewed at least annually or whenever significant organizational or operational changes occur.

6. Roles and Responsibilities:

SR. NO.	ROLE	RESPONSIBILITY
1.	Head, Accreditation / Approving Body (CEO)	Overall accountability for impartiality and ensuring effectiveness of this framework
2.	Impartiality Committee	Independent oversight of risk identification, review, and mitigation measures
3.	Quality Manager / MR	Maintenance of the Risk Register and coordination of reviews
4.	Assessors and Experts	Declaration of any conflict of interest before each assignment
5.	Governing Body	Periodic review of impartiality reports and endorsement of mitigation actions
6.	Secretariat / Accreditation Body Staff	Declaration / Annual Report and returns filing and submission asset record annually

6. Monitoring and Continual Improvement

- The Impartiality Committee meets at least once per year to review the impartiality risk assessment and recommend improvements.
- Outcomes of impartiality reviews are presented to the Management Committee and Governing Body for transparency and oversight.
- Lessons learned, complaints, or incidents of conflict of interest are analyzed to strengthen controls and update procedures.

7. Record and Documentation

All impartiality risk assessments, declarations, committee minutes, and corrective actions are recorded and retained in accordance with the Record Control Procedure (……).

These records serve as evidence of compliance and continuous improvement in impartiality management.

8. Conclusion:

Through this structured framework, M/s VISTA InfoSec ensures that impartiality risks are proactively identified, effectively mitigated, and continually monitored, thereby maintaining confidence, credibility, and international recognition of its accreditation and approval services.

Uncontrolled when printed, the approved version is held in the Certification Body document repository