IASCB-POL-007

Confidentiality & Information Security Policy

IASCB safeguards information received during accreditation activities while maintaining the transparency expected of a public-interest function.

Owner	Status	Review
IASCB Governance	Public policy	Annual or as required

Confidential information

Application records, assessment evidence, personnel information and commercially sensitive material are treated as confidential unless disclosure is authorised or required by law.

Access

Information is made available only to personnel, assessors, decision-makers and oversight bodies who require it for a defined IASCB activity.

Public information

Accredited status, certificate information and formal scopes may be published to support confidence and prevent misleading claims.

Security

IASCB uses reasonable administrative and technical controls to protect records against unauthorised access, alteration, loss or disclosure.

Retention

Records are retained for the period needed to demonstrate conformity, manage risks and meet legal or contractual obligations.

6. Data and access controls

IASCB shall request and retain information relevant to accreditation. Access shall be granted on a need-to-know basis for a defined role, use individual credentials where practicable, and be reviewed and removed promptly when no longer required.

7. Secure transfer and suppliers

Confidential evidence shall use controlled transfer channels and appropriate protection in storage. Cloud, IT, translation and other providers handling IASCB information shall be bound by confidentiality, security, continuity and incident-notification requirements.

8. Incidents and continuity

Suspected loss, unauthorised access, malware, accidental disclosure or material alteration shall be contained, investigated and recorded. Critical records shall be backed up, recoverable and periodically tested. This policy shall be reviewed annually and after significant incidents.