

ASF-GOV-004

Confidentiality Policy

Document code	ASF-GOV-004
Version	V3.0
Status	Published — effective 2026-12-01
Approved by	Prof. Giorgi Pkhakadze, MD, MPH, PhD President, Accréditation Sans Frontières
Applies to	All ASF personnel, surveyors, committee members, and any other persons with access to confidential information generated in ASF accreditation processes
Related documents	ASF-GOV-003 Impartiality Policy ASF-GOV-005 Complaints and Appeals Procedure ASF-OPS-001 Accreditation Decision Framework ASF-OPS-002 Surveyor Competency Policy ASF-QMS-003 Risk Management Policy
Legal framework	Regulation (EU) 2016/679 (GDPR) · Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (France) · Law of Georgia No. 5669 on Personal Data Protection
Supersedes	ASF-GOV-004 V2.0 (2026-11-20)
Next review	December 2031, or earlier on trigger

Version History

Version	Date	Nature of change	Approved by
V0.1	2026-10-26	Initial draft for internal review	—
V1.0	2026-11-09	President and Board review	ASF President
V2.0	2026-11-20	Approved and published	Prof. G. Pkhakadze, ASF President
V3.0	2026-12-01	Expanded to full policy; confidentiality classification table, data protection provisions (GDPR, French and Georgian law), data subject rights, breach response procedure, and references added	Prof. G. Pkhakadze, ASF President

1. Purpose

1.1 This policy establishes ASF's requirements for protecting confidential information generated in the course of its accreditation activities. Confidence in confidentiality is essential to the integrity of the accreditation process: applicants and accredited organisations must be able to share sensitive operational, clinical, and financial information with ASF surveyors and decision-makers, knowing that this information will be used solely for accreditation purposes and will not be disclosed without their consent.

1.2 This policy governs the confidentiality obligations of all persons who receive confidential information in the course of any ASF accreditation activity, including survey conduct, accreditation decision-making, standards development, appeals, and post-accreditation monitoring.

1.3 This policy is read alongside the ASF Impartiality Policy (ASF-GOV-003), which establishes related requirements for the non-disclosure of conflict-of-interest declarations.

2. Scope of Application

2.1 This policy applies to:

- (a) all ASF surveyors — Lead and Associate — during and after their surveys;
- (b) all members of the Accreditation Decision Committee (ADC), Standards Development Committee (SDC), and any other ASF committee or advisory body;
- (c) the ASF President and any delegated authority holder;
- (d) any external expert, peer reviewer, or consultant engaged by ASF;
- (e) any administrative or support staff with access to accreditation records.

2.2 The confidentiality obligation is effective from the moment a person receives confidential information and continues indefinitely after the end of their engagement with ASF, unless otherwise specified in this policy.

3. Classification of Confidential Information

3.1 For the purposes of this policy, confidential information is information that is not in the public domain and that was received by, or generated in the course of, ASF's accreditation activities. The following categories are classified as confidential by default:

Category	Specific information types
Applicant and accredited organisation information	All information provided by an applicant or accredited organisation in its application, self-assessment, or in the course of a survey, including: organisation structure, financial data, staffing levels, clinical performance data, incident records, complaint records, patient data, policy and procedure documents, and any other document submitted for assessment purposes.
Survey findings and process	All draft and final survey reports; surveyor field notes, observations, and working documents; nonconformance records; corrective action plan submissions and ASF's responses; survey schedules and itineraries; and any communications

Category	Specific information types
	between the survey team and the assessed organisation during and after the survey.
Accreditation decision information	The deliberations, discussions, and voting records of the Accreditation Decision Committee; draft accreditation decisions before formal issue; and all communications between ASF and the applicant or accredited organisation relating to the decision, unless and until the decision is formally communicated.
Standards development working materials	Unpublished draft standards and revisions; Standards Development Committee meeting minutes before formal approval and publication; consultation responses received from named stakeholders (unless the respondent consents to identification); expert review reports; and internal working documents of the SDC.
Personnel and governance records	Conflict-of-interest declarations; surveyor competency records and examination results; personnel files; committee member appointment records and deliberations; and any communication between ASF and individual surveyors or committee members relating to their performance or conduct.
Third-party information	Any information provided to ASF by a third party (regulatory body, peer accreditation organisation, or other source) under an expectation of confidence.

3.2 Where there is doubt as to whether specific information is confidential, it shall be treated as confidential until ASF confirms otherwise.

4. What Is Publicly Disclosed

4.1 ASF maintains a public registry of accreditation decisions. The following information is disclosed publicly for each accredited organisation, with the consent of the organisation or as a condition of accreditation:

- (a) the name and address of the accredited facility;
- (b) the ASF standard against which it was assessed;
- (c) the accreditation status (Accredited, Conditional Accreditation, or Recognition Award);
- (d) the accreditation effective dates (start date and next due date);
- (e) the ASF accreditation certificate number.

4.2 The following governance documents are publicly disclosed on france-asf.fr as part of ASF's transparency commitments:

- (a) all published ASF accreditation standards;
- (b) this policy and all other published ASF governance documents (GOV, OPS, QMS series);
- (c) the Standards Evidence Bibliography (ASF-EV-001);
- (d) the Stakeholder Consultation Summary (ASF-EV-002);
- (e) the Pilot and Field Validation Summary (ASF-EV-003);
- (f) the ISQua EEA Crosswalk (ASF-EV-004);
- (g) the ASF ISQua accreditation certificate (on receipt of ISQua EEA accreditation).

4.3 No information beyond that listed in clauses 4.1 and 4.2 is publicly disclosed without the express written consent of the relevant organisation or individual.

The distinction between public disclosure (clause 4.2) and confidentiality obligations (Section 3) is important for ISQua EEA compliance: ISQua Principle 3 (Transparency) requires that governance documents and standards are publicly available, while Principle 6 (Confidentiality) requires that assessment information is protected. Both requirements are met by ASF's information classification framework.

5. Confidentiality Obligations of Personnel

5.1 All persons subject to this policy are required to:

- (a) use confidential information only for the purpose for which it was received — that is, for the specific accreditation activity in connection with which it was provided;
- (b) not disclose confidential information to any third party without ASF's express written authorisation, except as required by law or legal process (see Section 7);
- (c) take reasonable precautions to prevent unauthorised access to confidential information, including appropriate handling of physical documents and secure storage of electronic information;
- (d) return or securely destroy confidential information on completion of their engagement, in accordance with ASF's records retention requirements (Section 8);
- (e) immediately report any suspected or actual breach of confidentiality to ASF (see Section 9).

5.2 These obligations apply during and after the period of engagement with ASF and do not expire. A surveyor who has completed their last survey, a committee member who has ended their term, and a consultant whose engagement has concluded remain bound by the confidentiality obligations of this policy in respect of any information received during their engagement.

5.3 Surveyors and committee members are reminded of their confidentiality obligations at each survey assignment and at each committee meeting as a standing agenda item.

6. Permitted Disclosures

6.1 Notwithstanding the general confidentiality obligations, the following disclosures are permitted:

- (a) Disclosure to ASF: surveyors and committee members may share confidential information within the ASF team as necessary to conduct accreditation activities, provided that the recipient is also subject to this policy;
- (b) Disclosure to ISQua EEA assessors: during an ISQua EEA assessment of ASF's own accreditation programme, ASF may provide ISQua assessors with access to anonymised or de-identified accreditation records as necessary to evidence compliance with EEA Principles. Information identifying individual facilities is not disclosed without consent;
- (c) Disclosure required by law or legal process: where a court order, regulatory notice, or applicable law requires disclosure of specific confidential information, ASF will disclose the minimum information required and will notify the affected organisation in advance where legally permitted to do so;

- (d) Disclosure with consent: where the person or organisation to whom the information relates provides express written consent to a specific disclosure, that disclosure is permitted within the scope of the consent;
- (e) Aggregate and anonymised data: ASF may use anonymised, aggregated data from its accreditation activities for research, quality improvement, or public reporting purposes, provided that no individual facility, surveyor, or committee member is identifiable from the published data.

6.2 All permitted disclosures under clause 6.1 are documented. Where the disclosure involves sharing information with a third party (other than ISQua EEA), the receiving party is required to agree to equivalent confidentiality obligations before receiving the information.

7. Data Protection and Personal Data

7.1 In the course of its accreditation activities, ASF processes personal data relating to healthcare facility personnel, surveyors, committee members, and potentially patients (for example, where patient records are reviewed as evidence during a survey). ASF processes such personal data in accordance with:

- (a) Regulation (EU) 2016/679 (the General Data Protection Regulation — GDPR), which applies to ASF's processing activities as a controller established in France;
- (b) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (the French Data Protection Act), as amended;
- (c) Law of Georgia No. 5669 on Personal Data Protection, where ASF processes personal data of Georgian data subjects.

7.2 The legal bases on which ASF processes personal data in its accreditation activities include:

- (a) performance of a contract — where personal data is processed in the course of carrying out an accreditation agreement with a facility or an engagement agreement with a surveyor or committee member;
- (b) legitimate interests — where ASF processes personal data to operate its accreditation programme and quality management system, in a manner that does not override the interests of the data subjects concerned;
- (c) compliance with a legal obligation — where applicable law requires retention of specific records.

7.3 ASF does not process special category personal data (including health data relating to individual patients) beyond what is strictly necessary for accreditation assessment purposes. Where patient data is reviewed during a survey, surveyors are instructed to note only what is necessary to assess the criterion in question and not to record identifying patient information in survey notes or reports.

7.4 Data subjects whose personal data is processed by ASF in the course of accreditation activities have the rights afforded by the GDPR, including the right to access, rectification, erasure (subject to legal retention requirements), and objection. Requests under these rights are addressed to ASF at the contact details on france-asf.fr. ASF responds within the timeframes required by applicable law.

7.5 ASF implements appropriate technical and organisational measures to protect personal data against unauthorised access, accidental loss, and unlawful processing. These measures are reviewed periodically and documented in the ASF Risk Management Policy (ASF-QMS-003).

ASF's principal operating jurisdictions are France (GDPR) and Georgia (Law No. 5669 on Personal Data Protection). Where ASF conducts surveys in other jurisdictions, it applies the higher of the applicable local data protection law and the GDPR standard.

8. Records Retention and Destruction

8.1 ASF retains confidential accreditation records for the following minimum periods:

Record type	Minimum retention period	Basis
Survey reports (final)	10 years from survey date	Accreditation programme record
Survey working notes and field records	5 years from survey date	Quality assurance and complaint response
Accreditation decision records (ADC minutes, decision letters)	10 years from decision date	Accreditation programme record
Conflict-of-interest declarations	5 years from activity date	Governance record
Confidentiality undertakings	5 years after end of engagement	Governance record
Standards development working documents (SDC minutes, consultation records, draft standards)	10 years from publication of the relevant standard	Evidence for ISQua EEA and future revisions
Complaint and appeal records	10 years from closure	Governance and legal
Personal data of facility personnel (processed during surveys)	5 years from survey date, subject to GDPR erasure rights	GDPR and programme record

8.2 At the end of the applicable retention period, confidential records are securely destroyed. Physical documents are shredded; electronic records are deleted and the relevant storage media is overwritten or destroyed. Destruction is documented in the ASF records destruction log.

8.3 Surveyors and committee members do not retain copies of confidential accreditation records beyond the period of their immediate engagement. On completion of a survey or committee term, any confidential documents held by the person are returned to ASF or securely destroyed, confirmed in writing.

9. Confidentiality Breach Response

9.1 A confidentiality breach is any actual or suspected unauthorised disclosure, access, loss, destruction, or alteration of confidential information held by ASF or by a person acting on its behalf.

9.2 Any person who suspects or becomes aware of a confidentiality breach must report it to the ASF President immediately — and in any event within 24 hours of becoming aware. Where the breach involves the President personally, it is reported to the SDC Chair.

9.3 On receipt of a breach report, ASF takes the following steps:

- (a) immediate containment — stopping any ongoing unauthorised disclosure and securing the affected information;
- (b) assessment — determining the nature and scope of the breach, the categories and volume of information affected, and the likely consequences for affected persons and organisations;
- (c) notification — notifying the affected organisation(s) without undue delay; and, where the breach involves personal data and meets the threshold in GDPR Article 33, notifying the relevant supervisory authority (the Commission Nationale de l'Informatique et des Libertés — CNIL — for France) within 72 hours;
- (d) remediation — implementing measures to prevent recurrence;
- (e) documentation — recording the breach, its assessment, notifications made, and remediation actions in the ASF breach register, retained as a controlled record.

9.4 Where a breach is attributable to a failure of an individual to comply with this policy, ASF applies the consequences set out in clause 9.5.

9.5 A person who intentionally discloses confidential accreditation information without authorisation is permanently removed from all ASF activities. A person whose negligent handling of confidential information results in a breach is subject to a formal warning and may be suspended pending a review of their competence to continue. Decisions under this clause may be appealed under ASF-GOV-005 (Complaints and Appeals Procedure).

10. ISQua EEA Alignment

10.1 This policy is designed to meet the confidentiality requirements of ISQua IAP EEA Principle 6 (Confidentiality), which requires that an accreditation programme has documented policies to protect the confidentiality of information obtained from assessed organisations. It also addresses the data protection requirements relevant to ASF's operating jurisdictions and the records management requirements supporting Principle 3 (Transparency) and Principle 5 (Review).

10.2 The ASF ISQua EEA Crosswalk (ASF-EV-004) maps the provisions of this policy to the applicable EEA criteria.

11. References

[1]	ISQua International Accreditation Programme (IAP). Principles for Standards. 6th Edition. ISQua External Evaluation Association, Dublin, Ireland, 2023.
[2]	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union, L 119, 4 May 2016.
[3]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (as amended). Légifrance, France.
[4]	Law of Georgia No. 5669 of 28 December 2011 on Personal Data Protection (as amended). Parliament of Georgia.
[5]	European Data Protection Board (EDPB). Guidelines 01/2021 on Examples Regarding Data Breach

	Notification. Version 1.0, 14 January 2021.
[6]	Commission Nationale de l'Informatique et des Libertés (CNIL). Guide RGPD pour les responsables de traitement. CNIL, Paris, 2022.
[7]	International Organization for Standardization. ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection: Information Security Management Systems. ISO, Geneva, 2022.
[8]	International Organization for Standardization. ISO/IEC 17021-1:2015 — Conformity Assessment: Requirements for Bodies Providing Audit and Certification of Management Systems. §5.3 Confidentiality. ISO, Geneva, 2015.
[9]	Joint Commission International. JCI Accreditation Standards for Hospitals. 7th Edition. JCI, Oak Brook, IL, 2020. (Section: Survey Process Confidentiality)
[10]	HQACI. Confidentiality Policy. ISQua EEA Accredited Document, 2026.
[11]	Shaw CD, Braithwaite J, Moldovan M, et al. Profiling health-care accreditation organisations: an international survey. Int J Qual Health Care. 2013;25(3):222–231.
[12]	Council of Europe. Convention 108+ — Convention for the Protection of Individuals with Regard to the Processing of Personal Data (modernised). Council of Europe, Strasbourg, 2018.

Formal Approval

Name and title	Signature	Date
Prof. Giorgi Pkhakadze, MD, MPH, PhD President, Accréditation Sans Frontières		2026-12-01

Document code: ASF-GOV-004 · Version: V3.0 · Effective: 2026-12-01 · Next review: December 2031