ACCRÉDITATION SANS FRONTIÈRES

ASF IT & Data Security Policy

Protecting the digital systems behind the public registry, complaint intake, and every ASF record

Version 2 · 2026
Paris · Geneva · Tbilisi

ASF-SECURITY-001-v2 · Published Paris, 12 September 2026 · Next review 12 September 2029

Document Control

Document Title	ASF IT & Data Security Policy
Document Reference	ASF-SECURITY-001-v2
Version / Edition	Version 2
Status	Published
Date of Publication	12 September 2026
Place of Publication	Paris, France
Issuing Authority	ASF International Standards Council, Accréditation Sans Frontières
Language of Origin	English
Effective Date	12 September 2026
Next Scheduled Review	12 September 2029
Supersedes	Version 1

Table of Contents

Foreword

Section 11 of How ASF Develops and Revises Standards addresses data protection and confidentiality of applicant information. The ASF Public Complaints & Feedback Policy addresses confidentiality of a complainant's identity. Neither treats information security as its own discipline — the actual technical and organizational controls protecting the systems that hold this data. DNV Healthcare's own NIAHO standards include a dedicated Security Management chapter, separate from general governance, for exactly this reason [1]. As ASF's public registry, complaint intake, and document repository move onto ASF's own website, this stops being a theoretical gap.

1. Purpose and Scope

This policy governs the security of ASF's own digital systems and the data they hold — the public accreditation registry, the complaint intake system, sentinel event records, and ASF's document repository — consistent with the information security management principles of ISO/IEC 27001 [2]. It does not restate the confidentiality obligations already stated elsewhere; it governs the technical and organizational controls that make those obligations actually enforceable in practice.

2. Why This Matters: The Real Cost of Getting This Wrong

This is not a theoretical concern. Healthcare has been the single costliest industry for data breaches for more than a decade running, with the average healthcare breach costing US$6.64 million in the most recent reporting year — more than any other sector measured [3]. Across Europe specifically, data protection authorities assessed nearly €1.2 billion in GDPR fines in a single recent year, with cumulative penalties since the regulation's introduction exceeding €7.1 billion [4].

The nature of the exposure matters as much as its cost. The average healthcare breach takes 279 days to identify and contain — well over a month longer than the cross-industry average — giving a genuine breach far more time to cause real harm before anyone notices it happened at all [5]. This is precisely why Section 6 of this policy treats detection speed, not only prevention, as a genuine, distinct requirement.

> *ASF is not a large hospital system, and does not hold the volume of data these industry-wide figures describe. But the underlying exposure — confidential survey findings, complainant identities, sentinel event reports — is exactly the category of data these statistics describe as most costly and most targeted. Scale changes the size of a potential incident; it does not change its basic nature.*

3. Data Classification

Every category of data ASF holds is classified consistent with the public/confidential distinction already established in Section 2 of the ASF Public Accreditation Registry Policy, extended here to cover ASF's full data holdings:

- Public — published standards, registry entries, and any document ASF has deliberately made publicly available; protected against unauthorized alteration, not against disclosure
- Confidential — survey findings, complainant identities, sentinel event reports, whistleblower reports, and personnel records; protected against both unauthorized alteration and unauthorized disclosure
- Restricted — the subset of confidential data carrying the highest sensitivity, including whistleblower reports under the ASF Internal Whistleblower Protection Policy and any data covered by special-category protections under Section 11 of How ASF Develops and Revises Standards; accessible only to the specific individuals whose role genuinely requires it

4. Access Control

Access to confidential or restricted data is granted only to individuals whose ASF function, under the ASF Personnel Competence & Awareness Policy, genuinely requires it, and is reviewed whenever that individual's function changes. Access is never granted by default to an entire team or role category where the actual work only requires a subset of that data.

5. Protection of Data in Transit and at Rest

Confidential and restricted data is encrypted both while stored and while transmitted — including data submitted through the public complaint intake system and the registry's own administrative interface — consistent with the technical safeguards ISO/IEC 27001 expects of an organization holding this category of information [2].

6. Security Incident Response

A security incident — unauthorized access, a data breach, or a genuine attempt at either — is treated as a distinct category from a patient safety sentinel event or a general internal nonconformity, though it is investigated with the same rigor as both. A security incident affecting confidential or restricted data is:

- Contained and assessed immediately upon discovery
- Where the incident involves personal data, reported to the competent data protection authority within seventy-two hours of ASF becoming aware of it, consistent with the real notification deadline the General Data Protection Regulation imposes on any organization processing personal data within the European Union [6]
- Investigated for root cause under the ASF Internal Nonconformity & Corrective Action Procedure
- Disclosed to any individual whose confidential data was genuinely affected, consistent with the data protection principles in Section 11 of How ASF Develops and Revises Standards

> *A data breach affecting a complainant's identity, or a whistleblower's, is not merely an IT problem — it is a direct failure of the specific protection this whole portfolio promises those two people by name. This policy treats it with that seriousness, not as a lesser, purely technical matter.*

7. The Human Factor

Across all industries, an estimated eighty-eight percent of data breaches trace back to human error — not a sophisticated external attack defeating strong technical defenses, but a mistake by someone with legitimate access [7]. This is precisely why this policy does not stand alone: competence in applying it is a required element of the ASF Personnel Competence & Awareness Policy for anyone performing a function under Section 4 of this policy, and awareness of why it matters — not only the rule itself — is treated as a genuine, distinct requirement under that policy's own Section 4.

References

[1] DNV. NIAHO® Accreditation Requirements, Interpretive Guidelines and Surveyor Guidance for Hospitals and Critical Access Hospitals, Revision 25-1. Høvik: DNV; 2025.

[2] International Organization for Standardization. ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva: ISO; 2022.

[3] Becker's Hospital Review, citing IBM Cost of a Data Breach Report 2026 (Ponemon Institute). Healthcare Data Breaches Cost $6.64M on Average. 2026.

[4] CNiC Solutions. Cybersecurity Compliance Statistics 2026: GDPR, HIPAA, PCI & CMMC Data. 2026.

[5] Fax Sip IT. Healthcare Cybersecurity Statistics: Breach Costs & Data in 2026. 2026.

[6] European Union. General Data Protection Regulation (EU) 2016/679, Article 33 (Notification of a Personal Data Breach to the Supervisory Authority). 2016.

[7] HIPAA Compliant Hosting. Healthcare Data Breach Statistics 2026: HIPAA Enforcement. 2026.

Annex A — Security Incident Record

Completed for every security incident identified under this policy.

Date discovered: _____

Systems or data affected: _____

☐ Public data

☐ Confidential data

☐ Restricted data

Containment

Action taken: _____

Date contained: _____

Regulatory Notification (if personal data affected)

Data protection authority notified on (within 72 hours): _____

Affected Individuals

☐ Notification required and completed

☐ No individual data genuinely affected

Root Cause

_____

Referred to Nonconformity Procedure on: _____

Index

Every protection this portfolio promises a patient, a complainant, or a whistleblower is only as real as the system holding their data. This policy is what makes that promise technically true, not just written down.