

Confidentiality and Access to Testing Material

GSQA-DAT-002 · 2.0 · 2026-10-19

1. Document classification

Complete originals, translations, notarisation and authentication documents, public extracts and internal verification findings are managed separately. Source, version, related subject and access rights must be clearly identified.

2. Upload and storage

Upload confirmation must correspond to actual storage, a file digest and the owning account. Private objects cannot be obtained merely by guessing a URL; the server checks identity and permissions for every request. Later drafts must not overwrite the formal submission snapshot.

3. Staff access

Access follows assignments and duties. Personnel with unresolved conflicts may not intervene. Downloads and status changes retain necessary audit records. Full private documents and credentials must not be written to public logs.

4. Incident response

If accidental publication, access-control problems or a file leak is discovered, access is restricted and evidence preserved first. The impact and notification or correction duties are assessed. Security statements must reflect actual capabilities, without claiming absolute security or unverifiable certification.

5. Submit complete reports

Provide the cover, every numbered page, methods, conditions, results, findings, limitations, attachments and revisions. Related failures, deviations, corrective action and retests must also be disclosed. Passing results cannot be selectively submitted.

6. Match the product and market configuration

Check the sample description, model, ratings, materials, critical components and software. A model-family report must state its coverage. Similar appearance alone does not justify extending findings.

7. Link clauses to measured results

For each award basis, record the standard and edition, clause, direction and unit of the limit, test conditions, measured result and report page. Resolve non-comparability or unresolved discrepancies before proceeding.

8. Assess whether reports remain valid

Check target-market time limits, standard editions and product changes. No uniform worldwide report-age limit is imposed. Original electronic files are preferred; scans must be complete and legible. An image of a seal does not establish a verified digital signature.

9. Preserve substantive test content

Public reports must contain result pages or charts that may lawfully be displayed, retaining the necessary scope, conditions and report identification. A cover does not replace substantive content. Complete private files, public extracts and redacted versions are managed separately.

10. Records, administration and correction

For matters covered by this document, records must retain the application or case number, specific product and market, version used, documents and page references, responsible personnel, material dates, reasons and formal notices. Personal information and trade secrets are handled according to access permissions. Questions about a record may be raised through correction, complaint or reconsideration channels available to an entitled applicant. Submission alone does not alter an existing decision or licence. The outcome is determined by the formal notice and current record.

11. Effective date, application and version control

Version 2.0 of this document is published and takes effect on 19 October 2026. It applies to relevant matters formally submitted after that date. Existing applications retain their original snapshot and rules. Material changes are notified separately and handled under transitional arrangements; new conditions are not retrospectively inserted into historical decisions. Website and downloadable texts must agree. Superseded versions identify their replacement, and name or wording corrections are recorded separately from substantive amendments.