Evidence Archive System – Customer/Audit Brief (EN) / ■■■■■■ – ■■/

Scope & Guarantee / ■■■■■
- This pack summarizes the configuration, controls, and validation outcomes for the Evidence Archive System.
- ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

1) Configuration Snapshot / ■■■■
- Secrets:
  - TASK_SECRET_TOKEN: sk_rotate_<random> (example: sk_rotate_Jj8pZrQf7w2A)
  - EVIDENCE_ROTATION_DAYS: 30
  - EVIDENCE_KEEP_MONTHLY: 1
- Storage: private directory 'evidence_bundles/' (NOT under /static)
- RBAC: Admin-only access for all evidence routes; rotation requires X-TASK-TOKEN.
- ■■■■■
  - ■■■■■■■■■■■■■
  - ■■■■■■■ 'evidence_bundles/'■■■■■ /static■■
  - ■■■■■■■■■■■■■■■■■■■■■■■■■■ X-TASK-TOKEN ■■■

2) Controls & Auditability / ■■■■■■■
- Admin RBAC enforced on: /admin/evidence, /downloads/evidence/*, /tasks/evidence/rotate
- Full audit logs for download/delete/rotation with IP + User-Agent + details.
- ■■■■■■■■■■■■■■/admin/evidence■/downloads/evidence/*■/tasks/evidence/rotate
- ■■/■■/■■■■■■■■■■■■IP■UA■■■■■

3) Operational Workflow / ■■■■
- Upload → Details → State-driven Next Steps (7-state FSM) — unchanged.
- Rotation policy: keep last 30 days; keep the first bundle of each month for long-term archival.
- ■■■■■■■■■■■■→■■→7■■■■■■■■■■■■■■30■■■■■■■■■■■■■

4) Validation Steps & Expected Results / ■■■■■■■■■■
4.1 Rotation trigger (should succeed) / ■■■■■■■■■■■
curl -X POST "https://<your-domain>/tasks/evidence/rotate" -H "X-TASK-TOKEN: sk_rotate_Jj8pZrQf7w2A" -H "Cookie: <AdminSessionCookie>"

Expected response / ■■■■■■
{"success": true, "kept":[...], "deleted":[...]}

4.2 Permission test (should fail) / ■■■■■■■■■■■
- Without token or non-admin → 401/403.

4.3 Integrity check / ■■■■■■
- Download /downloads/evidence/latest and verify any file's SHA256 matches `manifest.json`.
- ■■■■■ZIP■■■■■■■■■SHA256■ manifest.json ■■■■■■

4.4 Audit sampling / ■■■■■■SQL■
```
-- Recent 50 evidence ops
SELECT action, ip_address, user_agent, reason, created_at
FROM audit_logs
WHERE action IN ('evidence_download','evidence_delete','evidence_rotation')
ORDER BY created_at DESC
LIMIT 50;

-- Last 5 rotations
SELECT * FROM audit_logs
WHERE action='evidence_rotation'
ORDER BY created_at DESC
LIMIT 5;
```

5) Risk Notes / ■■■■
- Missing token or non-admin will be rejected by design.
- Ensure 'evidence_bundles/' is writable and never publicly exposed under /static.
- ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ /static ■■■

6) Acceptance Checklist (Tick ALL) / ■■■■■■■■■■■
[ ] TASK_SECRET_TOKEN configured; services restarted

[ ] Rotation returns {"success":true,"kept":...,"deleted":...}
[ ] Non-admin / no-token gets 401/403
[ ] SHA256 for any file equals manifest.json value
[ ] Audit logs contain download/delete/rotation (with IP/UA/details)
[ ] /admin/evidence bilingual texts OK; 3-color palette compliant
[ ] Main workflow unaffected

7) Attached Validation Evidence (Fill-in) / ■■■■■■■■
- Rotation Response JSON / ■■■■■
  { ...paste actual JSON here... }
- Latest ZIP sample SHA256 check / ■■ZIP■■■
  File: evidence_1_metrics_before.json
  SHA256 (manifest): <manifest sha256>
  SHA256 (local):   <local sha256>
  Result: MATCH / ■■
- Audit Log Excerpts / ■■■■■■■
  ... paste ...

8) Sign-off / ■■
- Prepared by / ■■■■_____   Date■_____
- Reviewed by / ■■■■_____   Date■_____
- Customer/Auditor Acknowledgement / ■■/■■■■■_____   Date■_____