NEXACC

IRS e-file Provider - Security & Privacy Self-Certification Support

NEXACC LLC - EFIN 868369 - IRS fiscal year 2026 - packet issued 2026-08-31
4750 S 44th Pl Suite 120, Phoenix, AZ 85040 - info@nexacc.com - +1 (443) 739-9197 - www.nexacc.com

This packet documents the controls behind each of the six security and privacy standards questions an Online Provider self-certifies, together with how an examiner can independently verify each one and which retained artifact supports it.

1. Extended Validation SSL Certificate

Certified: Yes

The site is served exclusively over HTTPS with a valid, publicly trusted TLS certificate covering the apex and www hosts. Plaintext HTTP is 301-redirected to HTTPS and HSTS is enforced sitewide (max-age 31536000, includeSubDomains). Certificates renew automatically ahead of expiry and validity is monitored.

Independent verification

- Browser padlock on https://www.nexacc.com/ shows the current certificate, issuer, and validity window.
- Certificate Transparency search for nexacc.com at https://crt.sh/?q=nexacc.com lists every certificate ever issued for the domain.
- Response headers on any page show strict-transport-security: max-age=31536000; includeSubDomains.

Retained artifact: Dated TLS scan output retained with the external vulnerability scan report.

2. External vulnerability scan

Certified: Yes

Automated external scan: TLS certificate chain and expiry, protocol redirect enforcement, HTTP security response headers, exposure of administrative and non-public routes, and dependency vulnerability scanning of the full software bill of materials. Recurring scan on a scheduled basis and after every significant release; critical findings are same-day work. Findings are triaged by severity, remediated, re-tested, and the report retained.

Independent verification

- Most recent scan: 2026-08-31. Scope: www.nexacc.com and nexacc.com (public web application), plus the application dependency SBOM.
- Open high or critical findings at that date: 0.
- Scan is reproducible on demand via the retained scan procedure; output is timestamped.

Retained artifact: Dated external vulnerability scan report plus remediation and re-test log.

3. Information privacy and safeguard policies

Certified: Yes

A written Information Security Plan built on IRS Publication 4557, IRS Publication 1345, and the FTC Safeguards Rule: a named security lead, annual risk assessment, least-privilege access with multi-factor authentication, encryption in transit and at rest, row-level database access controls, vendor due diligence, secure retention and disposal, and annual staff security training.

Independent verification

- Public privacy and safeguards commitments: https://www.nexacc.com/privacy
- IRC 7216 handling of tax return information and HIPAA Business Associate obligations are stated in that policy.

Retained artifact: Written Information Security Plan and the current annual risk assessment, provided to the IRS on request.

---

4. Web site challenge-response test

Certified: Yes

Every public form that collects contact details (contact, estimator, scheduling, onboarding entry) requires a challenge-response test a person can complete and an automated script cannot trivially pass. The challenge is plain text, works with keyboard and screen reader only, and is paired with silent bot traps and server-side validation. Failed attempts are rejected before any data is stored or emailed.

Independent verification

- Open https://www.nexacc.com/contact or the estimator and submit without answering the check: submission is refused.
- Challenge is rendered as accessible text, not an image puzzle, and is reachable by keyboard alone.

Retained artifact: Screenshots of the challenge on each public form plus the server-side rejection logic.

---

5. Public domain name registration

Certified: Yes

nexacc.com is registered through GoDaddy.com, LLC with publicly viewable registration data: registrar, creation and expiry dates, domain status codes, and authoritative name servers, all retrievable through ICANN's registration data lookup.

Independent verification

- ICANN registration data lookup: https://lookup.icann.org/en/lookup?q=nexacc.com
- Registrar GoDaddy.com, LLC; created 2021-08-21; expires 2027-08-21.
- Registrant contact is currently served through Domains By Proxy, LLC; the registrar privacy service is being switched off so the registrant organization publishes as NEXACC LLC.

Retained artifact: Dated registrar RDAP/WHOIS output retained with this packet.

---

6. Security incidents reporting

Certified: Yes

A documented incident response procedure: detect and contain, assess scope, preserve evidence, notify, remediate, and complete a written post-incident review. Confirmed or suspected incidents involving taxpayer data are reported to the IRS Stakeholder Liaison and, where applicable, the IRS

e-Help Desk, the FTC, state tax agencies, state attorneys general, and affected clients, without delay. HIPAA-covered incidents follow Breach Notification Rule timelines under our Business Associate Agreements.

Independent verification

- Public reporting channel and escalation steps: https://www.nexacc.com/security#report-an-incident
- Reports are acknowledged within one business day and tracked in an incident record.

Retained artifact: Incident response procedure document and the incident register (empty register is itself evidence).

Most recent external vulnerability scan

Date: 2026-08-31

Scope: www.nexacc.com and nexacc.com (public web application), plus the application dependency SBOM

Method: Automated external scan: TLS certificate chain and expiry, protocol redirect enforcement, HTTP security response headers, exposure of administrative and non-public routes, and dependency vulnerability scanning of the full software bill of materials.

Results

- TLS: valid publicly trusted certificate, current chain, automatic renewal ahead of expiry.
- Transport: all plaintext HTTP requests 301-redirect to HTTPS; HSTS enforced with max-age=31536000 and includeSubDomains.
- Headers: X-Content-Type-Options nosniff and Referrer-Policy strict-origin-when-cross-origin present on every response.
- Dependencies: no high or critical severity vulnerabilities in the application software bill of materials.
- Administrative routes: no unauthenticated access to admin, audit-log, or integration endpoints; database access is enforced by row-level security policies.

Open high or critical findings: 0. Recurring scan on a scheduled basis and after every significant release; critical findings are same-day work.

Domain registration record

Domain: nexacc.com

Registrar: GoDaddy.com, LLC

Created 2021-08-21 - expires 2027-08-21 - checked 2026-08-31

Name servers: NS49.DOMAINCONTROL.COM, NS50.DOMAINCONTROL.COM

Registry status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited

Registrant contact is currently served through Domains By Proxy, LLC; registrar privacy is being switched off so the registrant organization publishes as NEXACC LLC.

Public lookup: https://lookup.icann.org/en/lookup?q=nexacc.com

Where to find the supporting documents

Security program and incident reporting: https://www.nexacc.com/security

Privacy and safeguards policy: https://www.nexacc.com/privacy

IRS e-file Provider locator: https://www.irs.gov/e-file-providers/authorized-irs-e-file-provider-locator-service-for-tax-professionals

Attestation

The controls described above were in place at NEXACC LLC on the date this packet was issued. The written Information Security Plan, dated external vulnerability scan reports, remediation and re-test records, and the incident register are retained and provided to the IRS on request.

Signature: _____ Date: _____

Julius Ndahiro, Managing Partner & CFO, NEXACC LLC