

SYNTHETIC TEST DOCUMENT — FICTIONAL COMPANY — NO CUSTOMER DATA

Cedar Hollow Tax Services LLC

Written Information Security Plan (WISP)

Document ID	CHT-SEC-001
Version	2.0
Effective date	2026-09-01
Owner	Qualified Individual, Security Lead
Approved by	Managing Partners (approval minutes dated 2026-08-27)
Next scheduled review	2027-08-31, or sooner after a material change
Classification	Internal - synthetic test fixture

This document is a synthetic test fixture created for AuditReady page-count, pricing, and pre-scan testing. The company, people, vendors, and events are fictional. It contains no real customer data and no protected health information.

Test intent

A relatively detailed WISP with named owners, actions, timing, and evidence. It is a synthetic fixture, not proof that any real company follows these steps.

Revision history

Version	Date	Author (role)	Summary of change
1.0	2024-08-15	Security Lead	Initial WISP adopted by Managing Partners.
1.1	2025-01-20	Security Lead	Added annual risk assessment calendar and risk register fields.
1.2	2025-06-30	Operations Manager	Added MFA for remote access and quarterly access review form.
1.3	2026-02-10	Security Lead	Added FTC notification event evaluation step to incident response.
2.0	2026-09-01	Security Lead	Full restructure into SOPs; vendor oversight and disposal SOPs expanded; evidence index added.

Approval record

Approver (role)	Decision	Date	Evidence reference
Managing Partner A	Approved	2026-08-27	Partner meeting minutes MIN-2026-08
Managing Partner B	Approved	2026-08-27	Partner meeting minutes MIN-2026-08
Security Lead (Qualified Individual)	Owner sign-off	2026-08-25	Signed cover memo CHT-MEMO-114

Contents

- 1. Purpose and scope
- 2. Roles and responsibilities
- 3. Information and system inventory
- 4. Risk assessment SOP
- 5. Access control SOP
- 6. Authentication, encryption, and device rules
- 7. Change management and secure configuration
- 8. Monitoring and logging
- 9. Training and testing SOP
- 10. Vendor oversight SOP
- 11. Incident response SOP
- 12. Retention and secure disposal SOP
- 13. Backup and business continuity
- 14. Governance, annual report, and evidence
- 15. Glossary
- Appendix A - Annual compliance calendar
- Appendix B - Responsibility matrix (RACI)
- Appendix C - Forms and log fields
- Appendix D - Retention schedule
- Appendix E - Service provider register
- Appendices F onward - Control evidence records

1. Purpose and scope

Cedar Hollow is a fictional tax preparer and electronic return originator. This information security program covers taxpayer data, tax return information, client portal records, paper files, laptops, cloud services, and vendors that handle customer information. The program is designed to protect the security, confidentiality, and integrity of customer information, to protect against reasonably anticipated threats or hazards, and to protect against unauthorized access that could result in substantial harm or inconvenience to any customer.

The Security Lead is designated as the Qualified Individual responsible for overseeing, implementing, and enforcing this information security program. The Security Lead maintains a system and data inventory and reviews this WISP every year and after material changes, such as a new office, a new tax software platform, a merger, or a security event.

1.1 Information in scope

Information type	Examples	Formats
Taxpayer identity data	Names, SSNs, ITINs, dates of birth, identity document images	Electronic, paper
Tax return information	Draft and filed returns, schedules, e-file acknowledgements	Electronic, paper
Financial account data	Refund deposit account and routing numbers, payment records	Electronic
Client portal records	Uploaded source documents, secure messages, signature records	Electronic
Engagement records	Engagement letters, consent forms, preparer notes	Electronic, paper

1.2 Systems and locations in scope

- Main office and seasonal satellite office (fictional addresses on file with Operations).
- Tax preparation software (hosted, fictional platform 'LedgerLine Tax').
- Client portal (fictional platform 'PortalVault') and business email tenant.
- Managed Windows laptops, the file server, network equipment, and printers or scanners that store images.
- Cloud backup service and off-site records storage vendor.
- Any service provider that receives, maintains, processes, or accesses customer information.

1.3 Out of scope

Personal devices are out of scope only because they are prohibited from storing taxpayer data. Marketing website content that never receives customer information is out of scope but is still covered by change management.

2. Roles and responsibilities

Role	Responsibilities
Security Lead (Qualified Individual)	Owns the WISP, risk assessment, control testing, incident response coordination, vendor reviews, and the annual written report to the Managing Partners.
Managing Partners	Approve the WISP, risk exceptions, budget, and the annual report; receive escalations for material security events.
Operations Manager	Approves access requests based on job need; reports role changes within one business day; owns onboarding and offboarding checklists.
IT Administrator	Implements access changes, MFA, encryption, patching, logging, backups, and device sanitization; disables departing staff accounts on the departure date.
Records Manager	Maintains the retention schedule, legal holds, disposal log, and vendor destruction certificates.
Procurement	Performs service provider due diligence before contract signature and keeps contract security clauses current.
All staff	Complete training, follow this WISP, protect credentials, and report suspected incidents immediately.

3. Information and system inventory

The Security Lead maintains an inventory of data, personnel, devices, systems, and facilities that store or process customer information. Each inventory entry records the system owner, data types, location, hosting model, encryption status, MFA status, backup status, and the date it was last verified.

- The inventory is verified each January as an input to the risk assessment.
- New systems are added before go-live as part of the change management checklist.
- Retired systems are moved to a retired list with the sanitization or destruction evidence reference.
- Data flow diagrams for the client portal, e-file submission, and backups are reviewed annually.

4. Risk assessment SOP

Each January, the Security Lead documents reasonably foreseeable internal and external risks, assesses likelihood and impact, identifies controls, and records residual risk in the risk register. New software, vendors, or workflows require a risk review before launch. Managing Partners approve any risk exception, with an owner and expiration date.

4.1 Procedure

- Step 1 - Confirm the system and data inventory is current.
- Step 2 - Identify threats: phishing, credential theft, ransomware, lost devices, insider misuse, vendor compromise, misdirected mail, and physical theft.
- Step 3 - Rate likelihood and impact from 1 (low) to 5 (high) using the matrix in 4.2.
- Step 4 - Record existing controls and evaluate whether they sufficiently address each risk.
- Step 5 - Record residual risk, the treatment decision (mitigate, accept, transfer, avoid), owner, and target date.
- Step 6 - Present results to the Managing Partners in the annual report and track treatments to closure.

4.2 Scoring matrix

Score (L x I)	Rating	Required action
1-4	Low	Accept or treat during normal operations; review annually.
5-9	Moderate	Treatment plan with owner and target date within 90 days.
10-16	High	Treatment plan within 30 days; Managing Partners informed.
17-25	Critical	Immediate treatment; Managing Partners approve any interim exception in writing.

4.3 Risk exceptions

A risk exception records the risk, compensating controls, business reason, owner, approval by the Managing Partners, and an expiration date no more than twelve months out. Expired exceptions are closed or re-approved.

5. Access control SOP

Only named accounts may access customer information. The Operations Manager approves access based on job need and least privilege. The Security Lead reviews access rights quarterly; managers report role changes within one business day. IT disables departing staff accounts on their departure date. Shared accounts are prohibited.

- Provisioning: access request form, Operations Manager approval, IT implementation, confirmation logged.
- Privileged access: administrator accounts are separate from daily accounts and require MFA and Security Lead approval.
- Quarterly review: system owners attest to each account; exceptions are removed within five business days.
- Offboarding: accounts disabled on the departure date, devices returned, badge and keys collected, checklist signed.
- Physical access: file rooms are locked; visitors sign in and are escorted.

6. Authentication, encryption, and device rules

Multi-factor authentication is required for all staff access to the client portal, email, remote access, and systems containing customer information. Customer information is encrypted at rest on managed laptops and servers and encrypted in transit with TLS. IT records encryption exceptions, applies compensating controls, and obtains written approval from the Security Lead before use. Unmanaged devices may not store taxpayer data.

- Passwords or passphrases of at least 14 characters; password manager provided to all staff.
- Full-disk encryption verified monthly through the device management console.
- Screens lock after 10 minutes; lost devices are reported immediately and remotely wiped.
- Removable media is blocked by default; approved encrypted drives are logged.

7. Change management and secure configuration

Changes to systems that store or process customer information follow a documented change procedure: request, risk review, approval by the system owner, testing, implementation window, and post-change verification. Secure baseline configurations are maintained for laptops, the file server, firewalls, and cloud tenants, and deviations are recorded.

8. Monitoring and logging

IT monitors authorized user activity and detects unauthorized access, use of, or tampering with customer information. Logs from email, the client portal, the tax platform, endpoint protection, and the firewall are retained for at least one year. Alerts are reviewed each business day during tax season and at least weekly otherwise.

9. Training and testing SOP

Employees complete security awareness training at hire and annually. The Security Lead performs quarterly phishing exercises and documents follow-up coaching. Vulnerability scans run monthly; a qualified independent tester performs an annual penetration test. The Security Lead tracks findings to closure and verifies fixes.

Activity	Frequency	Owner	Evidence
Security awareness training	At hire and annually	Security Lead	Training completion log
Phishing simulation	Quarterly	Security Lead	Campaign results and coaching notes
Vulnerability scan	Monthly	IT Administrator	Scan report and remediation tickets
Penetration test	Annually	Independent tester	Test report and retest letter
Security staff updates	Ongoing	Security Lead	Continuing education records

10. Vendor oversight SOP

Before a service provider receives customer information, Procurement documents due diligence on its safeguards and incident response. Contracts require appropriate security controls and prompt incident notice. The Security Lead reviews critical providers annually and records remediation for material gaps.

- Tiering: critical (stores or processes customer information), important, and low.
- Due diligence: security questionnaire, independent assurance report where available, breach history, and insurance.
- Contract terms: safeguards, confidentiality, incident notice, return or destruction of data, and right to assess.
- Annual review: critical providers re-assessed; findings logged with owner and due date.

11. Incident response SOP

Staff report suspected unauthorized access immediately to the Security Lead. The incident response team preserves evidence, contains affected accounts, assesses what customer information was involved, coordinates recovery, and records decisions in an incident log. Legal counsel determines any applicable customer or regulator notice obligations, including whether an event involving unencrypted information of 500 or more consumers must be reported to the FTC no later than 30 days after discovery. The team conducts a lessons-learned review within 30 days of closure.

- Phase 1 - Report and triage (immediately).
- Phase 2 - Contain and preserve evidence (same day).
- Phase 3 - Assess scope and information involved.
- Phase 4 - Notify as determined by legal counsel.
- Phase 5 - Recover and verify.
- Phase 6 - Lessons learned within 30 days of closure; update this WISP.

12. Retention and secure disposal SOP

The Records Manager keeps a retention schedule by record type and documents legal holds. When retention expires, paper containing customer information is cross-cut shredded by an approved vendor; electronic copies are securely erased or destroyed. Vendor destruction certificates are retained. Exceptions require a documented legal or business reason and a review date. Backups follow the approved deletion schedule. Customer information is disposed of no later than two years after the last date it was used to provide a product or service, unless retention is required by law or a legitimate business need documented in the retention schedule.

13. Backup and business continuity

Backups of the file server and tax platform exports run nightly, are encrypted, and are stored off-site with the cloud backup provider. Restore tests run quarterly and results are logged. The continuity plan covers loss of the office, loss of the tax platform during filing season, and ransomware recovery.

14. Governance, annual report, and evidence

The Security Lead gives the Managing Partners a written annual report covering risk assessment results, control testing, security events, vendor status, and recommended changes. Evidence records include access reviews, training logs, scan results, incident logs, disposal certificates, and approval minutes.

15. Glossary

Term	Meaning in this WISP
Customer information	Any record containing nonpublic personal information about a customer, in any format.
Qualified Individual	The person designated to oversee, implement, and enforce the information security program (the Security Lead).
Service provider	Any third party that receives, maintains, processes, or accesses customer information.
MFA	Multi-factor authentication: at least two of knowledge, possession, or inherence factors.
Encryption	Transformation of data so it is unreadable without a key; at rest and in transit.
Security event	An event resulting in unauthorized access to, or disruption or misuse of, an information system or information.
Notification event	Acquisition of unencrypted customer information without authorization, as evaluated by legal counsel.
Legal hold	An instruction suspending disposal of records relevant to litigation or investigation.
Residual risk	Risk remaining after controls are applied.

Appendix A - Annual compliance calendar

Month	Activities
January	Risk assessment; inventory verification; access review Q1
February	Phishing exercise Q1; monthly vulnerability scan
March	Restore test Q1; tax-season monitoring cadence review
April	Access review Q2; post-season device check
May	Phishing exercise Q2; annual vendor reviews begin
June	Penetration test; restore test Q2
July	Access review Q3; retention schedule review
August	Phishing exercise Q3; WISP annual review and partner approval
September	Annual security training; restore test Q3
October	Access review Q4; disposal event and certificate collection
November	Phishing exercise Q4; continuity tabletop exercise
December	Annual written report to Managing Partners; restore test Q4

Appendix B - Responsibility matrix (RACI)

Activity	Security Lead	Partners	Ops Mgr	IT	Records
Risk assessment	R/A	I	C	C	C
Access approval	C	-	R/A	R	-
Quarterly access review	A	I	R	R	-
MFA and encryption	A	-	-	R	-
Training and phishing	R/A	I	C	C	-
Vendor due diligence	A	I	C	C	C
Incident response	R/A	I	C	R	C

Activity	Security Lead	Partners	Ops Mgr	IT	Records
Secure disposal	A	-	-	R	R
Annual report	R	A	C	C	C

Appendix C - Forms and log fields

C.1 Access request form

- Requester name and role
- Systems and permission level requested
- Business justification
- Operations Manager approval and date
- IT implementation date and ticket reference
- Review due date

C.2 Incident log

- Incident ID and date reported
- Reporter and detection source
- Systems and customer information involved
- Containment actions and times
- Legal counsel notice determination
- Closure date and lessons-learned reference

C.3 Disposal log

- Disposal event ID and date
- Record types and approximate volume
- Method (cross-cut shred, secure erase, physical destruction)
- Vendor name and certificate number
- Witness or verifier
- Legal hold check completed (yes or no)

Appendix D - Retention schedule

Record type	Retention period	Disposal method	Owner
Filed tax returns and workpapers	Per legal guidance, documented by record type	Cross-cut shred / secure erase	Records Manager
Client source documents (copies)	Return to client or dispose after filing season review	Cross-cut shred	Records Manager
Engagement letters and consents	Per legal guidance	Secure erase	Records Manager
Portal uploads	Purged per approved schedule	Platform purge + verification	IT Administrator
Backups	Rolling schedule	Automatic expiry verified quarterly	IT Administrator
Retired devices	Until sanitized	NIST-style purge or physical destruction	IT Administrator

Appendix E - Service provider register

Provider (fictional)	Service	Tier	Last review	Status
LedgerLine Tax	Tax preparation platform	Critical	2026-05	No open findings
PortalVault	Client portal	Critical	2026-05	One finding closed 2026-06
SkyKeep Backup	Cloud backup	Critical	2026-06	No open findings

Provider (fictional)	Service	Tier	Last review	Status
ShredRight Services	Paper destruction	Important	2026-07	Certificates current
NorthPoint IT	Managed IT support	Critical	2026-04	Contract clauses updated

Appendix F.001 - Control evidence checklist item: Annual risk assessment

Control area	Annual risk assessment
Requirement reference	16 CFR 314.4(b)
Scope for this record	Main office file server
Control owner	Security Lead
Frequency	Annually (January)
Review period	2025-10
Evidence required	Signed risk register, scoring worksheets, partner review minutes
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-10, the Security Lead performed the annual risk assessment control for the main office file server in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (annually (january)), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Signed risk register saved to the evidence folder for 2025-10.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the main office file server are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0001. This record is part of a synthetic test fixture for a fictional company.

Appendix F.002 - Control evidence checklist item: Quarterly access review

Control area	Quarterly access review
Requirement reference	16 CFR 314.4(c)(1)
Scope for this record	Seasonal satellite office
Control owner	Security Lead
Frequency	Quarterly
Review period	2026-05
Evidence required	Account attestation per system, removal tickets, reviewer sign-off
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-05, the Security Lead performed the quarterly access review control for the seasonal satellite office in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (quarterly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Account attestation per system saved to the evidence folder for 2026-05.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the seasonal satellite office are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0002. This record is part of a synthetic test fixture for a fictional company.

Appendix F.003 - Control evidence checklist item: Data and system inventory

Control area	Data and system inventory
Requirement reference	16 CFR 314.4(c)(2)
Scope for this record	Records storage vendor
Control owner	Security Lead
Frequency	Annually and on change
Review period	2025-12
Evidence required	Inventory export with verification dates
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-12, the Security Lead performed the data and system inventory control for the records storage vendor in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (annually and on change), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Inventory export with verification dates saved to the evidence folder for 2025-12.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the records storage vendor are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0003. This record is part of a synthetic test fixture for a fictional company.

Appendix F.004 - Control evidence checklist item: Encryption at rest

Control area	Encryption at rest
Requirement reference	16 CFR 314.4(c)(3)
Scope for this record	Business email tenant
Control owner	IT Administrator
Frequency	Monthly verification
Review period	2026-07
Evidence required	Device console encryption report, exception register
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-07, the IT Administrator performed the encryption at rest control for the business email tenant in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (monthly verification), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Device console encryption report saved to the evidence folder for 2026-07.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the business email tenant are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0004. This record is part of a synthetic test fixture for a fictional company.

Appendix F.005 - Control evidence checklist item: Encryption in transit

Control area	Encryption in transit
Requirement reference	16 CFR 314.4(c)(3)
Scope for this record	Scanner and multifunction printers
Control owner	IT Administrator
Frequency	Quarterly
Review period	2026-02
Evidence required	TLS configuration scan, portal and email settings capture
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-02, the IT Administrator performed the encryption in transit control for the scanner and multifunction printers in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (quarterly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: TLS configuration scan saved to the evidence folder for 2026-02.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the scanner and multifunction printers are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0005. This record is part of a synthetic test fixture for a fictional company.

Appendix F.006 - Control evidence checklist item: Secure development and configuration

Control area	Secure development and configuration
Requirement reference	16 CFR 314.4(c)(4)
Scope for this record	Client portal (PortalVault, fictional)
Control owner	IT Administrator
Frequency	On change
Review period	2026-09
Evidence required	Baseline configuration records and deviation log
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-09, the IT Administrator performed the secure development and configuration control for the client portal (portalvault, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (on change), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Baseline configuration records and deviation log saved to the evidence folder for 2026-09.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the client portal (portalvault, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0006. This record is part of a synthetic test fixture for a fictional company.

Appendix F.007 - Control evidence checklist item: Multi-factor authentication

Control area	Multi-factor authentication
Requirement reference	16 CFR 314.4(c)(5)
Scope for this record	Cloud backup (SkyKeep, fictional)
Control owner	IT Administrator
Frequency	Monthly
Review period	2026-04
Evidence required	MFA enrollment report for all accounts with customer information access
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-04, the IT Administrator performed the multi-factor authentication control for the cloud backup (skykeep, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (monthly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: MFA enrollment report for all accounts with customer information access saved to the evidence folder for 2026-04.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the cloud backup (skykeep, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0007. This record is part of a synthetic test fixture for a fictional company.

Appendix F.008 - Control evidence checklist item: Secure disposal of customer information

Control area	Secure disposal of customer information
Requirement reference	16 CFR 314.4(c)(6)
Scope for this record	Managed IT support provider (NorthPoint, fictional)
Control owner	Records Manager
Frequency	Per retention schedule
Review period	2025-11
Evidence required	Disposal log, vendor certificates of destruction
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-11, the Records Manager performed the secure disposal of customer information control for the managed IT support provider (northpoint, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (per retention schedule), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Disposal log saved to the evidence folder for 2025-11.
- Evidence item 2: owner sign-off by the Records Manager with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section.

Follow-up and escalation

If this control fails or evidence is missing, the Records Manager opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the managed IT support provider (northpoint, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Records Manager (performed) and Security Lead (reviewed). Record ID CHT-EV-0008. This record is part of a synthetic test fixture for a fictional company.

Appendix F.009 - Control evidence checklist item: Change management

Control area	Change management
Requirement reference	16 CFR 314.4(c)(7)
Scope for this record	Managed laptops - preparer pool
Control owner	IT Administrator
Frequency	On change
Review period	2026-06
Evidence required	Change tickets with approval, test, and verification notes
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-06, the IT Administrator performed the change management control for the managed laptops - preparer pool in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (on change), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Change tickets with approval saved to the evidence folder for 2026-06.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the managed laptops - preparer pool are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0009. This record is part of a synthetic test fixture for a fictional company.

Appendix F.010 - Control evidence checklist item: Activity monitoring and logging

Control area	Activity monitoring and logging
Requirement reference	16 CFR 314.4(c)(8)
Scope for this record	Remote access gateway
Control owner	IT Administrator
Frequency	Daily in season / weekly
Review period	2026-01
Evidence required	Alert review log, log retention configuration
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-01, the IT Administrator performed the activity monitoring and logging control for the remote access gateway in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (daily in season / weekly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Alert review log saved to the evidence folder for 2026-01.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the remote access gateway are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0010. This record is part of a synthetic test fixture for a fictional company.

Appendix F.011 - Control evidence checklist item: Penetration testing

Control area	Penetration testing
Requirement reference	16 CFR 314.4(d)(2)
Scope for this record	Tax platform (LedgerLine Tax, fictional)
Control owner	Security Lead
Frequency	Annually
Review period	2026-08
Evidence required	Independent test report, remediation tracker, retest letter
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-08, the Security Lead performed the penetration testing control for the tax platform (ledgerline tax, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (annually), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Independent test report saved to the evidence folder for 2026-08.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the tax platform (ledgerline tax, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0011. This record is part of a synthetic test fixture for a fictional company.

Appendix F.012 - Control evidence checklist item: Vulnerability scanning

Control area	Vulnerability scanning
Requirement reference	16 CFR 314.4(d)(2)
Scope for this record	Paper file room
Control owner	IT Administrator
Frequency	Monthly
Review period	2026-03
Evidence required	Scan reports and closure evidence
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-03, the IT Administrator performed the vulnerability scanning control for the paper file room in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (monthly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Scan reports and closure evidence saved to the evidence folder for 2026-03.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the paper file room are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0012. This record is part of a synthetic test fixture for a fictional company.

Appendix F.013 - Control evidence checklist item: Security awareness training

Control area	Security awareness training
Requirement reference	16 CFR 314.4(e)
Scope for this record	Main office file server
Control owner	Security Lead
Frequency	At hire and annually
Review period	2025-10
Evidence required	Training completion log with dates
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-10, the Security Lead performed the security awareness training control for the main office file server in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (at hire and annually), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Training completion log with dates saved to the evidence folder for 2025-10.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the main office file server are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0013. This record is part of a synthetic test fixture for a fictional company.

Appendix F.014 - Control evidence checklist item: Phishing exercises

Control area	Phishing exercises
Requirement reference	16 CFR 314.4(e)
Scope for this record	Seasonal satellite office
Control owner	Security Lead
Frequency	Quarterly
Review period	2026-05
Evidence required	Campaign results, coaching notes
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-05, the Security Lead performed the phishing exercises control for the seasonal satellite office in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (quarterly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Campaign results saved to the evidence folder for 2026-05.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the seasonal satellite office are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0014. This record is part of a synthetic test fixture for a fictional company.

Appendix F.015 - Control evidence checklist item: Service provider oversight

Control area	Service provider oversight
Requirement reference	16 CFR 314.4(f)
Scope for this record	Records storage vendor
Control owner	Procurement
Frequency	Before onboarding and annually
Review period	2025-12
Evidence required	Due diligence file, contract clauses, annual review record
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-12, the Procurement performed the service provider oversight control for the records storage vendor in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (before onboarding and annually), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Due diligence file saved to the evidence folder for 2025-12.
- Evidence item 2: owner sign-off by the Procurement with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time.

Follow-up and escalation

If this control fails or evidence is missing, the Procurement opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the records storage vendor are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Procurement (performed) and Security Lead (reviewed). Record ID CHT-EV-0015. This record is part of a synthetic test fixture for a fictional company.

Appendix F.016 - Control evidence checklist item: WISP evaluation and adjustment

Control area	WISP evaluation and adjustment
Requirement reference	16 CFR 314.4(g)
Scope for this record	Business email tenant
Control owner	Security Lead
Frequency	Annually and after material change
Review period	2026-07
Evidence required	Redlined WISP and approval minutes
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-07, the Security Lead performed the wisp evaluation and adjustment control for the business email tenant in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (annually and after material change), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Redlined WISP and approval minutes saved to the evidence folder for 2026-07.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the business email tenant are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0016. This record is part of a synthetic test fixture for a fictional company.

Appendix F.017 - Control evidence checklist item: Incident response plan

Control area	Incident response plan
Requirement reference	16 CFR 314.4(h)
Scope for this record	Scanner and multifunction printers
Control owner	Security Lead
Frequency	Tested annually
Review period	2026-02
Evidence required	Plan, tabletop record, incident log
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-02, the Security Lead performed the incident response plan control for the scanner and multifunction printers in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (tested annually), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Plan saved to the evidence folder for 2026-02.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the scanner and multifunction printers are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0017. This record is part of a synthetic test fixture for a fictional company.

Appendix F.018 - Control evidence checklist item: Annual written report to Managing Partners

Control area	Annual written report to Managing Partners
Requirement reference	16 CFR 314.4(i)
Scope for this record	Client portal (PortalVault, fictional)
Control owner	Security Lead
Frequency	Annually (December)
Review period	2026-09
Evidence required	Signed report and partner acknowledgement
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-09, the Security Lead performed the annual written report to managing partners control for the client portal (portalvault, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (annually (december)), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Signed report and partner acknowledgement saved to the evidence folder for 2026-09.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the client portal (portalvault, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0018. This record is part of a synthetic test fixture for a fictional company.

Appendix F.019 - Control evidence checklist item: FTC notification event evaluation

Control area	FTC notification event evaluation
Requirement reference	16 CFR 314.4(j)
Scope for this record	Cloud backup (SkyKeep, fictional)
Control owner	Legal counsel
Frequency	Per event
Review period	2026-04
Evidence required	Counsel determination memo, submission record if required
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-04, the Legal counsel performed the ftc notification event evaluation control for the cloud backup (skykeep, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (per event), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Counsel determination memo saved to the evidence folder for 2026-04.
- Evidence item 2: owner sign-off by the Legal counsel with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged.

Follow-up and escalation

If this control fails or evidence is missing, the Legal counsel opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the cloud backup (skykeep, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Legal counsel (performed) and Security Lead (reviewed). Record ID CHT-EV-0019. This record is part of a synthetic test fixture for a fictional company.

Appendix F.020 - Control evidence checklist item: Backup and restore testing

Control area	Backup and restore testing
Requirement reference	Continuity control
Scope for this record	Managed IT support provider (NorthPoint, fictional)
Control owner	IT Administrator
Frequency	Quarterly
Review period	2025-11
Evidence required	Restore test log with result and duration
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-11, the IT Administrator performed the backup and restore testing control for the managed IT support provider (northpoint, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (quarterly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Restore test log with result and duration saved to the evidence folder for 2025-11.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the managed IT support provider (northpoint, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0020. This record is part of a synthetic test fixture for a fictional company.

Appendix F.021 - Control evidence checklist item: Offboarding account disablement

Control area	Offboarding account disablement
Requirement reference	16 CFR 314.4(c)(1)
Scope for this record	Managed laptops - preparer pool
Control owner	IT Administrator
Frequency	On departure date
Review period	2026-06
Evidence required	Offboarding checklist and disable timestamp
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-06, the IT Administrator performed the offboarding account disablement control for the managed laptops - preparer pool in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (on departure date), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Offboarding checklist and disable timestamp saved to the evidence folder for 2026-06.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the managed laptops - preparer pool are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0021. This record is part of a synthetic test fixture for a fictional company.

Appendix F.022 - Control evidence checklist item: Physical security of file rooms

Control area	Physical security of file rooms
Requirement reference	16 CFR 314.4(c)(1)
Scope for this record	Remote access gateway
Control owner	Operations Manager
Frequency	Monthly walkthrough
Review period	2026-01
Evidence required	Walkthrough checklist and key log
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-01, the Operations Manager performed the physical security of file rooms control for the remote access gateway in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (monthly walkthrough), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Walkthrough checklist and key log saved to the evidence folder for 2026-01.
- Evidence item 2: owner sign-off by the Operations Manager with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period.

Follow-up and escalation

If this control fails or evidence is missing, the Operations Manager opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the remote access gateway are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Operations Manager (performed) and Security Lead (reviewed). Record ID CHT-EV-0022. This record is part of a synthetic test fixture for a fictional company.

Appendix F.023 - Control evidence checklist item: Removable media control

Control area	Removable media control
Requirement reference	16 CFR 314.4(c)(3)
Scope for this record	Tax platform (LedgerLine Tax, fictional)
Control owner	IT Administrator
Frequency	Monthly
Review period	2026-08
Evidence required	Blocked device report, approved drive log
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-08, the IT Administrator performed the removable media control control for the tax platform (ledgerline tax, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (monthly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Blocked device report saved to the evidence folder for 2026-08.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the tax platform (ledgerline tax, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0023. This record is part of a synthetic test fixture for a fictional company.

Appendix F.024 - Control evidence checklist item: Retention schedule review

Control area	Retention schedule review
Requirement reference	16 CFR 314.4(c)(6)
Scope for this record	Paper file room
Control owner	Records Manager
Frequency	Annually (July)
Review period	2026-03
Evidence required	Approved schedule with change notes
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-03, the Records Manager performed the retention schedule review control for the paper file room in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (annually (july)), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Approved schedule with change notes saved to the evidence folder for 2026-03.
- Evidence item 2: owner sign-off by the Records Manager with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review.

Follow-up and escalation

If this control fails or evidence is missing, the Records Manager opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the paper file room are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Records Manager (performed) and Security Lead (reviewed). Record ID CHT-EV-0024. This record is part of a synthetic test fixture for a fictional company.

Appendix F.025 - Control evidence checklist item: Annual risk assessment

Control area	Annual risk assessment
Requirement reference	16 CFR 314.4(b)
Scope for this record	Main office file server
Control owner	Security Lead
Frequency	Annually (January)
Review period	2025-10
Evidence required	Signed risk register, scoring worksheets, partner review minutes
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-10, the Security Lead performed the annual risk assessment control for the main office file server in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (annually (january)), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Signed risk register saved to the evidence folder for 2025-10.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the main office file server are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0025. This record is part of a synthetic test fixture for a fictional company.

Appendix F.026 - Control evidence checklist item: Quarterly access review

Control area	Quarterly access review
Requirement reference	16 CFR 314.4(c)(1)
Scope for this record	Seasonal satellite office
Control owner	Security Lead
Frequency	Quarterly
Review period	2026-05
Evidence required	Account attestation per system, removal tickets, reviewer sign-off
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-05, the Security Lead performed the quarterly access review control for the seasonal satellite office in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (quarterly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Account attestation per system saved to the evidence folder for 2026-05.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the seasonal satellite office are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0026. This record is part of a synthetic test fixture for a fictional company.

Appendix F.027 - Control evidence checklist item: Data and system inventory

Control area	Data and system inventory
Requirement reference	16 CFR 314.4(c)(2)
Scope for this record	Records storage vendor
Control owner	Security Lead
Frequency	Annually and on change
Review period	2025-12
Evidence required	Inventory export with verification dates
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-12, the Security Lead performed the data and system inventory control for the records storage vendor in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (annually and on change), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Inventory export with verification dates saved to the evidence folder for 2025-12.
- Evidence item 2: owner sign-off by the Security Lead with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section.

Follow-up and escalation

If this control fails or evidence is missing, the Security Lead opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the records storage vendor are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Security Lead (performed) and Security Lead (reviewed). Record ID CHT-EV-0027. This record is part of a synthetic test fixture for a fictional company.

Appendix F.028 - Control evidence checklist item: Encryption at rest

Control area	Encryption at rest
Requirement reference	16 CFR 314.4(c)(3)
Scope for this record	Business email tenant
Control owner	IT Administrator
Frequency	Monthly verification
Review period	2026-07
Evidence required	Device console encryption report, exception register
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-07, the IT Administrator performed the encryption at rest control for the business email tenant in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (monthly verification), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Device console encryption report saved to the evidence folder for 2026-07.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the business email tenant are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0028. This record is part of a synthetic test fixture for a fictional company.

Appendix F.029 - Control evidence checklist item: Encryption in transit

Control area	Encryption in transit
Requirement reference	16 CFR 314.4(c)(3)
Scope for this record	Scanner and multifunction printers
Control owner	IT Administrator
Frequency	Quarterly
Review period	2026-02
Evidence required	TLS configuration scan, portal and email settings capture
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-02, the IT Administrator performed the encryption in transit control for the scanner and multifunction printers in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (quarterly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: TLS configuration scan saved to the evidence folder for 2026-02.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the scanner and multifunction printers are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0029. This record is part of a synthetic test fixture for a fictional company.

Appendix F.030 - Control evidence checklist item: Secure development and configuration

Control area	Secure development and configuration
Requirement reference	16 CFR 314.4(c)(4)
Scope for this record	Client portal (PortalVault, fictional)
Control owner	IT Administrator
Frequency	On change
Review period	2026-09
Evidence required	Baseline configuration records and deviation log
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-09, the IT Administrator performed the secure development and configuration control for the client portal (portalvault, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (on change), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Baseline configuration records and deviation log saved to the evidence folder for 2026-09.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status. Where a service provider performs the control, the provider's attestation and the contract clause reference are attached. The reviewer noted that the procedure in this WISP was followed as written and did not require an update this period. The control result is summarized in the annual written report to the Managing Partners under the control testing section. Training records show that staff with access to taxpayer data completed the required module before access was granted. Disposal evidence for this period includes the vendor certificate of destruction and the internal disposal log entry. MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the client portal (portalvault, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0030. This record is part of a synthetic test fixture for a fictional company.

Appendix F.031 - Control evidence checklist item: Multi-factor authentication

Control area	Multi-factor authentication
Requirement reference	16 CFR 314.4(c)(5)
Scope for this record	Cloud backup (SkyKeep, fictional)
Control owner	IT Administrator
Frequency	Monthly
Review period	2026-04
Evidence required	MFA enrollment report for all accounts with customer information access
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2026-04, the IT Administrator performed the multi-factor authentication control for the cloud backup (skykeep, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (monthly), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: MFA enrollment report for all accounts with customer information access saved to the evidence folder for 2026-04.
- Evidence item 2: owner sign-off by the IT Administrator with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

MFA enrollment was confirmed for every account in scope, including administrator and service accounts with interactive access. The reviewer sampled five records from the period and traced each one to the supporting ticket or log entry without exception. Change tickets affecting this control were reviewed to confirm that the system owner approved the change before implementation. Monitoring alerts related to this control were reviewed within the cadence stated in the monitoring and logging section. The service provider register was checked to confirm that any vendor involved in this control has a current annual review. The Managing Partners were informed of no material weaknesses for this control in the current period. Retention of this evidence follows the retention schedule in Appendix D, and the evidence is not subject to a legal hold. The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day.

Follow-up and escalation

If this control fails or evidence is missing, the IT Administrator opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the cloud backup (skykeep, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: IT Administrator (performed) and Security Lead (reviewed). Record ID CHT-EV-0031. This record is part of a synthetic test fixture for a fictional company.

Appendix F.032 - Control evidence checklist item: Secure disposal of customer information

Control area	Secure disposal of customer information
Requirement reference	16 CFR 314.4(c)(6)
Scope for this record	Managed IT support provider (NorthPoint, fictional)
Control owner	Records Manager
Frequency	Per retention schedule
Review period	2025-11
Evidence required	Disposal log, vendor certificates of destruction
Status	Operating as designed - evidence on file

Procedure performed

For the review period 2025-11, the Records Manager performed the secure disposal of customer information control for the managed IT support provider (northpoint, fictional) in accordance with the Cedar Hollow WISP. The control owner gathered the required evidence, compared it against the documented procedure and frequency (per retention schedule), and recorded any deviation in the exception register. The Security Lead, as Qualified Individual, reviewed the completed record, confirmed that customer information within the scope remained protected, and signed the record. Findings, if any, were assigned an owner and a due date and tracked to closure in the remediation tracker referenced by this appendix.

Evidence checklist

- Evidence item 1: Disposal log saved to the evidence folder for 2025-11.
- Evidence item 2: owner sign-off by the Records Manager with date recorded.
- Evidence item 3: Security Lead (Qualified Individual) review signature and date.
- Evidence item 4: exception register checked; new exceptions approved by the Managing Partners with an expiration date.
- Evidence item 5: risk register entry updated to reflect current residual risk.
- Evidence item 6: result carried forward to the annual written report to the Managing Partners.

Reviewer notes

The independent tester's most recent report did not include findings that affect this control. Restore testing confirmed that backups covering this scope could be recovered within the target recovery time. The Operations Manager confirmed that role changes for staff in this scope were reported within one business day. The reviewer confirmed that the evidence matches the frequency stated in the WISP and that the owner signed the record. Any exception identified during the review was entered in the exception register with an owner, compensating control, and expiration date. The Security Lead verified that remediation items from the prior period were closed and that closure evidence is attached. Customer information remained encrypted at rest and in transit for the systems covered by this record during the review period. Access to the evidence folder is limited to the Security Lead, the Managing Partners, and the external assessor when engaged. No shared accounts were identified; named accounts were confirmed against the current staff roster provided by the Operations Manager. The record was cross-referenced to the risk register entry so that residual risk ratings reflect the current control status.

Follow-up and escalation

If this control fails or evidence is missing, the Records Manager opens a remediation item within five business days, rates the gap using the scoring matrix in Section 4.2, and notifies the Security Lead. High or critical gaps affecting the managed IT support provider (northpoint, fictional) are reported to the Managing Partners within 30 days, and any related security event is handled under the incident response SOP in Section 11. Closure requires retest evidence.

Sign-off: Records Manager (performed) and Security Lead (reviewed). Record ID CHT-EV-0032. This record is part of a synthetic test fixture for a fictional company.