Information Security and Technology Risk Addendum

This Information Security and Technology Risk Addendum (this "Addendum") is entered into as of January 15, 2026 (the "Addendum Effective Date") by and between Redwood Peak Financial, Inc., a Delaware corporation ("Company"), and Nimbus Ridge Technologies, LLC, a California limited liability company ("Vendor"). This Addendum is incorporated into and forms part of the Master Services Agreement dated January 10, 2026 (the "Agreement"). Capitalized terms not defined in this Addendum have the meanings given in the Agreement.

1. Order of Precedence

If there is a conflict between this Addendum and the Agreement relating to information security, confidentiality, privacy, audit, incident response, or audit/assurance deliverables, this Addendum controls for that subject matter.

2. Scope and Covered Environments

2.1 **Scope.** This Addendum applies to Vendor's provision of the services described in the Agreement (the "Services") and to all systems, networks, applications, endpoints, facilities, personnel, and Subprocessors used to store, process, transmit, or otherwise access Company Data (the "In-Scope Environment").

2.2 **Service Description (semi-structured).** The parties intend the following summary to describe the operational scope for security purposes (to be updated as needed by written agreement):

Field	Value
Service name	NimbusVault Cloud File Collaboration
Service type	SaaS
Hosting model	Multi-tenant
Hosting provider(s)	Amazon Web Services (AWS)
Primary regions	US-West (Oregon), US-East (N. Virginia)
Authorized data locations	United States only
Customer/admin access method	SSO (SAML 2.0) and local administrative accounts (restricted)
Support model	24x7 for Sev 1/Sev 2; business hours for general tickets
Production access	Restricted; just-in-time elevation via bastion and approval workflow
Subprocessors (high level)	AWS (hosting), Twilio (SMS), SendGrid (email), Sentry (error monitoring)

2.3 **Data Categories (semi-structured).** The parties classify Company Data as follows:

Data Category	Included? (Y/N)	Examples	Special Handling
Business confidential	Y	pricing, contracts, internal financial reports	encrypt at rest/in transit; limited access
Personal Information	Y	employee names, emails, phone numbers	access logs; least privilege; breach notice
Sensitive Personal Information	N	SSN, precise geolocation	not permitted; block/filters where feasible
Credentials/secrets	Y	API tokens for SSO provisioning, admin recovery codes	vaulting; rotation; restricted viewing
Payment card data (PCI)	N	PAN, cardholder data	not permitted
Health data (PHI)	N	medical records	not permitted
Source code	N	repos, build artifacts	not applicable
Other regulated data	N	none	not applicable

2.4 In-Scope Components and Records (semi-structured). For clarity in audit and IRM reviews, the following components and records are included in-scope to the extent they store, process, transmit, or provide administrative access to Company Data:

Component/Record Type	Included In-Scope?	Notes
Production application services	Y	NimbusVault production workloads
Production databases/storage	Y	object storage and relational DB
Identity provider and SSO integration	Y	SAML SSO + admin auth
Bastion/jump host / ZTNA gateway	Y	administrative pathway
End-user devices used for administration	Y	Vendor-admin managed devices only

Component/Record Type	Included In-Scope?	Notes
Security logs (auth, admin, data access)	Y	see Section 11 and Section 12
Backups and snapshots	Y	retention and deletion rules apply
Non-production environments	Y (limited)	must not contain Company Data except as expressly approved in writing

3. Definitions

3.1 **"Company Data"** means all data or information (including Personal Information) that Company or its customers/users provides or makes available to Vendor, or that Vendor accesses, collects, receives, stores, transmits, generates, or processes on Company's behalf in connection with the Agreement, including authentication data, keys/tokens, and security telemetry relating to Company's environment.

3.2 **"Personal Information"** has the meaning in applicable privacy law, including the California Consumer Privacy Act, as amended ("CCPA").

3.3 **"Security Incident"** means any actual or reasonably suspected (a) unauthorized access to, acquisition of, disclosure of, alteration of, loss of, or destruction of Company Data; (b) compromise of Vendor's or Subprocessor's In-Scope Environment; (c) ransomware, extortion, or malware event impacting the Services or Company Data; or (d) material weakness that is reasonably likely to result in (a)–(c).

3.4 **"Security Documentation"** means Vendor policies, procedures, standards, audit/certification reports, summaries of penetration tests, vulnerability management metrics, incident response plans, BC/DR plans, and other materials reasonably necessary to validate compliance with this Addendum.

3.5 **"Subprocessor"** means any third party (including Vendor Affiliates) that processes Company Data on Vendor's behalf.

3.6 **"Confidential Information"** includes Company Data and any Security Documentation or findings exchanged under this Addendum.

3.7 **"Risk Acceptance"** means Company's written acceptance of a defined security risk associated with a documented noncompliance with this Addendum, subject to (a) a defined scope, (b) compensating controls, (c) a time-bound remediation plan, and (d) an expiration date.

3.8 **"Vendor Personnel"** means Vendor employees, contractors, and agents who access Company Data or administer the In-Scope Environment.

3.9 **"Authentication Data"** means passwords, passphrases, MFA secrets, recovery codes, API tokens, session tokens, and cryptographic keys used to authenticate or authorize access.

4. Security Governance and Program Requirements

4.1 **Security Program.** Vendor will maintain and follow a written information security program aligned to recognized standards (e.g., ISO/IEC 27001, NIST CSF, or equivalent), appropriate to the Services and Company Data.

4.2 **Security Ownership.** Vendor will maintain a designated security leader responsible for oversight of the program and for compliance with this Addendum.

4.3 **Policy Framework.** Vendor will maintain policies and procedures addressing, at minimum: asset management; access control; cryptography; physical and environmental security; operations security; communications security; secure development (if applicable); supplier relationships; incident management; business continuity; records management; and compliance.

4.4 **Risk Assessment.** Vendor will perform and document risk assessments at least annually and upon material changes to the In-Scope Environment.

4.5 **Exception Management.** Vendor will maintain an exception process for deviations from security standards (including Exhibit G), with documented business justification, risk assessment, compensating controls, owner approval, and planned remediation dates.

5. Control Baseline and Minimum Security Requirements

5.1 **Baseline.** Vendor will implement and maintain safeguards designed to protect confidentiality, integrity, and availability of Company Data, including the minimum controls in this Addendum and the Security Schedule in Exhibit G.

5.2 **No Material Degradation.** Vendor will not materially reduce the effectiveness of safeguards applicable to Company Data during the Term.

5.3 **Control Objectives.**

Objective	Outcome
Confidentiality	Company Data accessed only by authorized users for authorized purposes
Integrity	Company Data and systems protected from unauthorized modification
Availability	Services resilient; recovery processes meet agreed objectives
Accountability	Actions affecting Company Data traceable via logs and controls

6. Identity, Access, Authentication, and Password Management

6.1 **Least Privilege.** Vendor will implement least-privilege access and role-based access controls (RBAC) for the In-Scope Environment.

6.2 **MFA.** Vendor will enforce multi-factor authentication (MFA) for (a) privileged accounts, (b) remote access, and (c) all access to production environments.

6.3 **Privileged Access Management.** Vendor will control and monitor privileged access, including: (a) prohibiting shared privileged accounts except where technically necessary and logged; (b) implementing just-in-time access or time-bound elevation where feasible; and (c) logging privileged session activity.

6.4 **Account Lifecycle.** Vendor will revoke access within 24 hours after personnel termination or role change that removes the need for access.

6.5 **Access Reviews.** Vendor will conduct privileged access reviews at least quarterly and general access reviews at least semi-annually.

6.6 Password Management Standard. Vendor will maintain and enforce a written password standard for any password-based authentication used for the Services or the In-Scope Environment (including administrative accounts and "break-glass" accounts). At a minimum, Vendor will: (a) require passwords/passphrases of at least 14 characters for administrative accounts and at least 12 characters for other accounts, or, where supported, enforce equivalent strength via modern authentication controls; (b) prohibit the use of default vendor passwords and prohibit known-compromised passwords through screening controls; (c) require secure storage of passwords using salted hashing for any stored credentials and prohibit plaintext storage; (d) implement account lockout or rate limiting to mitigate brute force attacks; (e) prohibit password sharing, and prohibit reuse of privileged passwords across systems; (f) store administrative passwords and recovery codes only in a centralized approved vault with access logging; and (g) rotate "break-glass" credentials at least every 90 days and upon any suspected compromise or personnel change affecting authorized custodians.

6.7 Authentication and Authorization Protocols. Vendor will use modern protocols for authentication and authorization for the Services as follows: (a) **End-user authentication.** SAML 2.0 SSO is supported and is the default for Company; local user accounts (if enabled) must enforce MFA and password controls consistent with Section 6.6. (b) **API authentication.** API access will use OAuth 2.0 bearer tokens or signed tokens, with scoped permissions and configurable expiration. (c) **Administrative access.** Administrative access to production will occur only via the approved bastion/secure gateway with MFA and session logging. (d) **Authorization.** Vendor will enforce RBAC within the application and administrative tooling and will document the role model for Company upon request.

Authentication/Authorization Summary Table.

Access Type	Protocol/Method	MFA Required	Authorization Model	Logging
End-user UI	SAML 2.0 SSO	Y	RBAC (tenant roles)	auth + role changes
Local UI accounts (if enabled)	password + MFA	Y	RBAC	auth + role changes
API access	OAuth 2.0 tokens	N/A (token-based)	scopes/claims	token issuance + API calls (where feasible)
Vendor admin to production	bastion + MFA	Y	least privilege + JIT elevation	session logs + admin actions

7. Encryption and Key Management

7.1 **Encryption.** Vendor will encrypt Company Data in transit and at rest.

7.2 Data in Transit Requirements (TLS). Vendor will enforce encryption in transit for all external and internal transmissions of Company Data over untrusted networks, including: (a) Company-to-Service connections (web and API); (b) Service-to-Subprocessor transmissions (e.g., email/SMS providers) to the extent they carry Company Data; and (c) administrative connections to production systems. Vendor will use TLS 1.2 or higher (TLS 1.3 where feasible), will not knowingly enable insecure cipher suites, and will manage certificates using documented procedures.

7.3 **Key Rotation.** Vendor will rotate encryption keys at least annually and upon suspected compromise.

7.4 **Secrets Management.** Vendor will use a centralized secrets vault and prohibit hardcoding secrets.

Crypto/Key "chart".

Item	Requirement	Minimum Standard
TLS	In transit encryption	TLS 1.2+ (prefer 1.3)
At rest	Storage encryption	AES-256 (or equivalent)
Key access	Restricted	least privilege + MFA
Key rotation	Regular	annual + on compromise
Secret storage	Centralized	KMS-backed secrets vault

8. Network Security, Segmentation, and Malware Protection

8.1 **Segmentation.** Vendor will segment environments to reduce blast radius (e.g., separate production from non-production, restrict east-west traffic).

8.2 **Remote Administration.** Vendor will restrict administrative access through controlled pathways (e.g., bastion hosts, secure jump boxes, ZTNA), with MFA and logging.

8.3 Malware Protection (EDR/Anti-Malware). Vendor will implement and maintain malware protection controls appropriate to the In-Scope Environment, including: (a) endpoint detection and response (EDR) or anti-malware on all Vendor-managed endpoints used to administer production and on in-scope servers where feasible; (b) automatic signature/agent updates and tamper protection; (c) alerting to security operations for malware detections and suspicious execution; (d) documented response procedures, including isolation/quarantine, eradication, and post-incident review; and (e) periodic verification of agent coverage for in-scope endpoints.

Malware/EDR Coverage Table (contractual minimums).

Asset Type	Coverage Requirement	Monitoring/Alerting	Evidence Example
Vendor admin workstations	100% EDR coverage	real-time alerts	EDR console coverage report
Bastion/jump hosts	EDR where feasible	real-time alerts	host agent inventory
Production servers/containers	malware controls appropriate to platform	alerting integrated	security tooling summary

Asset Type	Coverage Requirement	Monitoring/Alerting	Evidence Example
Email ingress/egress (Vendor)	anti-phishing/malware filtering	alerting + quarantine	email security settings

9. IT Asset Management and Secure Configuration

9.1 **Asset Inventory.** Vendor will maintain an inventory of in-scope assets, including cloud accounts/subscriptions, production workloads, databases, and security tooling. The inventory will identify environment (prod/non-prod), owner, and criticality.

9.2 **Inventory Review.** Vendor will review and reconcile the in-scope asset inventory at least quarterly and upon material changes.

9.3 **Secure Configuration Baselines.** Vendor will maintain secure configuration baselines (e.g., CIS benchmarks or equivalent) for in-scope systems and will remediate material drift in a timely manner.

Asset Inventory Minimum Fields (semi-structured).

Field	Example
Asset ID	aws-prod-eks-01
Asset type	Kubernetes cluster
Environment	Production
Data sensitivity	Company Data (Confidential + Personal Information)
Owner	Platform Engineering
Region	us-west-2
Last reviewed	Dec 31, 2025

10. Secure Development and Change Management (if applicable)

Vendor will maintain secure SDLC practices and change management for production changes affecting Company Data.

11. Vulnerability Management

Vendor will scan for vulnerabilities, remediate based on risk, and meet the remediation SLAs in Exhibit G.

12. Logging, Monitoring, Records Management, and Retention

12.1 **Logging.** Vendor will collect and retain security-relevant logs for systems processing Company Data, including authentication, authorization, privileged actions, and access to production data where feasible.

12.2 **Log Retention.** Vendor will retain security logs for at least 180 days, unless a longer period is required by law or mutually agreed for a specific investigation or legal hold.

12.3 **Monitoring.** Vendor will monitor for anomalous activity and maintain alerting for material events affecting Company Data.

12.4 Records Management. Vendor will maintain a records management program covering Company Data, Security Documentation, and security logs, including: (a) documented retention periods and disposal methods; (b) procedures to preserve records subject to legal hold or investigation; (c) access controls and auditability for records; and (d) deletion and disposal consistent with Section 13 (Return/Deletion) and Exhibit G (DATA controls).

Records Retention Schedule (sample, contractual minimums).

Record Type	Minimum Retention	Storage Location (typical)	Notes
Security logs (auth/admin/data access)	180 days	SIEM/log platform	extend for investigations/legal holds
Incident reports and RCA	3 years	GRC/IR repository	includes corrective actions
Access review evidence	2 years	GRC repository	privileged reviews quarterly
Asset inventory snapshots	2 years	CMDB exports	quarterly reviews
Subprocessor diligence artifacts	3 years	vendor management repository	contracts, reports summaries

13. Data Minimization; Hosting Location; Retention; Return/Deletion

13.1 **Minimization.** Vendor will collect and process only the minimum Company Data necessary to perform the Services.

13.2 Hosting Location Commitment. Vendor will store and process Company Data only in the United States (including primary hosting, disaster recovery, backups, and log storage), and will not relocate Company Data outside the United States without Company's prior written consent.

13.3 Location Controls. Vendor will maintain technical and organizational controls designed to enforce the hosting location commitment, including: region restrictions within cloud accounts, configuration guardrails/policies, and periodic review of data residency settings.

13.4 **Return and Export.** Upon termination or expiration, Vendor will make Company Data available for export for 30 days in a commercially reasonable format.

13.5 **Deletion.** Vendor will securely delete Company Data from active systems within 60 days after the export period ends or Company requests deletion, except for legal retention and backups.

13.6 **Backups.** If Company Data remains in backups, Vendor will protect it under this Addendum and delete it per backup rotation schedules.

13.7 **Deletion Certification.** Upon request, Vendor will certify deletion in writing.

Data Lifecycle Flow (chart).

Stage	Description	Control
Ingest	data received/created	validation + encryption
Use	processing for Services	RBAC + logging
Share	Subprocessor transfers	transfer approval; contract flow-down
Store	at rest	encryption + segmentation
Archive	backups	access restricted + rotation
Dispose	deletion	secure wipe + certification

14. Subprocessors and Fourth Parties

Vendor will flow down obligations to Subprocessors, remain responsible for their acts and omissions, and provide 30 days' notice for new Subprocessors with a 15-day objection period.

15. Incident Response and Breach Notification

Vendor will maintain and test an incident response plan annually and will notify Company within 72 hours after becoming aware of a Security Incident, provide ongoing updates, and deliver a written incident report within 10 business days after containment.

16. Business Continuity and Disaster Recovery

Vendor will maintain and annually test BC/DR plans meeting the RPO/RTO targets below:

Component	RPO	RTO
Core service	24 hours	48 hours
Identity	8 hours	24 hours
Logs	24 hours	72 hours

17. Audit, Assurance, and Compliance Support

Vendor will maintain an annual SOC 2 Type II report covering the In-Scope Environment (or ISO/IEC 27001 certification as an acceptable alternative), provide reports upon request, and support targeted audits in the event of a Security Incident or material breach.

18. Regulatory Requests and Legal Holds

Vendor will notify Company of legally binding requests for Company Data (unless prohibited) and comply with

Company legal holds to the extent lawful.

19. Financial Responsibility; Incident Costs; Insurance

Vendor will reimburse Company for reasonable response costs for Security Incidents caused by Vendor breach, negligence, or willful misconduct, and will maintain $5,000,000 cyber/privacy insurance.

20. Remedies; Equitable Relief

Company may seek injunctive relief. If Vendor's security posture presents an imminent risk to Company Data, Company may require Vendor to suspend affected processing until mitigated.

21. Term; Survival

This Addendum continues for the Term of the Agreement. Vendor's obligations survive termination or expiration for as long as Vendor retains Company Data.

Exhibit A — Control Matrix (Detailed)

Vendor will maintain controls that meet or exceed the following minimum requirements for the In-Scope Environment.

Control Domain	Control Requirement	Minimum Standard	Evidence Examples
Governance	Written security program	aligned to ISO/NIST	policies; security charter
Asset Mgmt	inventory of in-scope assets	quarterly reviewed	CMDB export; tagging reports
Access	RBAC + least privilege	enforced	IAM policies; access reviews
MFA	MFA for privileged/prod	required	IdP settings
Password Mgmt	password standard + vault	per Section 6.6	password policy; vault logs
AuthN/AuthZ	modern protocols + RBAC	per Section 6.7	SSO config; role model
Crypto	encrypt at rest/in transit	TLS 1.2+; AES-256	configs; KMS policies
Secrets	vaulting + rotation	no hardcoding	vault logs; scan reports
Patch	patching cadence	risk-based	patch reports
Vuln Mgmt	scanning + SLAs	per Exhibit G	scan + ticket exports
Monitoring	centralized logs + alerting	implemented	SIEM dashboards
Malware	EDR/anti-malware	per Section 8.3	EDR coverage reports

Control Domain	Control Requirement	Minimum Standard	Evidence Examples
Network	segmentation + secure admin	bastion + logging	diagrams; session logs
Records	retention + legal hold	per Section 12.4	retention schedule
Backup	tested backups	annual test min	test summary
Incident	tested IR plan	annual tabletop	tabletop report
Training	annual awareness	required	completion records
Subprocessors	flow-down contracts	required	contract excerpts
Data Location	US-only commitment	enforced	region guardrails evidence

Exhibit B — Security Metrics Pack (Quarterly) (Sample Data Structure)

Metric	Definition	Q1	Q2	Q3	Q4
Critical vulns past SLA	# open critical vulns older than SLA	0	1	0	0
High vulns past SLA	# open high vulns older than SLA	3	2	1	2
Patch compliance	% assets patched within policy	96%	95%	97%	96%
MFA coverage	% privileged accounts with MFA	100%	100%	100%	100%
EDR coverage (admin endpoints)	% admin endpoints reporting healthy agent	100%	99%	100%	100%
Password vault usage	% privileged credentials stored in vault	100%	100%	100%	100%
IR tabletop completion	tabletop performed?	Y	N	N	Y

Exhibit C — Data Flow and Control Mapping (Text Chart)

Step	Data Movement	Example	Control Points
1	Company → Service ingress	API upload	TLS; auth; rate limiting
2	Ingress → Application	request processing	RBAC; input validation

Step	Data Movement	Example	Control Points
3	Application → Database	store records	encryption at rest; access logs
4	Application → Subprocessor	SMS/email alerts	TLS; transfer approval; subprocessor contract
5	Application → Logs/SIEM	audit events	centralized logging; retention
6	Backup/Archive	snapshots	restricted access; rotation
7	Export/Delete	termination	export window; secure deletion

Exhibit D — Subprocessor Register (Expanded)

Subprocessor	Service	Data Categories	Regions	Certs/Reports	Breach Notice to Vendor	Contract Flow-down Confirmed
Amazon Web Services, Inc.	hosting/compute/storage	business confidential; Personal Information; credentials/secrets	United States	SOC 1/2/3; ISO/IEC 27001	48 hours	Y
Twilio Inc.	SMS notifications	Personal Information (phone numbers)	United States	SOC 2 Type II	48 hours	Y
SendGrid, Inc.	email delivery	Personal Information (emails); business confidential (message content)	United States	SOC 2 Type II	48 hours	Y
Functional Software, Inc. (Sentry)	error monitoring	limited telemetry; user identifiers (where configured)	United States	SOC 2 Type II	72 hours	Y

Exhibit E — Security Contacts (Semi-Structured)

Role	Name/Title	Email	Phone	Escalation Hours
Vendor Security POC	Maya Chen, Director of Information Security	security@nimbusridge.example	+1 (415) 555-0142	24x7
Vendor Legal POC	Daniel R. Price, Senior Counsel	legal@nimbusridge.example	+1 (415) 555-0199	Business hours

Role	Name/Title	Email	Phone	Escalation Hours
Company Security POC	Alicia Gomez, Head of Cyber Risk	cyberrisk@redwoodpeak.example	+1 (415) 555-0108	24x7
Company Legal POC	Jordan Patel, Associate General Counsel	legal@redwoodpeak.example	+1 (415) 555-0120	Business hours

Exhibit F — Compliance Mapping Worksheet (Sample)

Internal Requirement ID	Requirement Summary	Contract Reference	Evidence	Status
IRM-IAM-001	MFA required for all privileged and production access	Section 6.2; Exhibit G (IAM-01/IAM-02)	SSO enforcement export; bastion MFA config	Compliant
IRM-PASS-003	Password vaulting + break-glass rotation	Section 6.6; Exhibit G (PASS-01/PASS-02)	vault access logs; rotation record	Compliant
IRM-ASSET-001	Quarterly in-scope asset inventory	Section 9.1–9.2; Exhibit G (ASSET-01)	CMDB export	Compliant
IRM-LOG-004	Security logs retained at least 180 days	Section 12.2; Exhibit G (LOG-02)	SIEM retention config	Compliant
IRM-RES-002	Records retention schedule maintained	Section 12.4	retention schedule	Compliant
IRM-ENC-002	TLS enforced for Company Data	Section 7.2; Exhibit G (CRYP-01)	TLS configuration evidence	Compliant
IRM-LOC-001	US-only data residency	Section 13.2–13.3; Exhibit G (LOC-01)	region policy evidence	Compliant
IRM-MAL-001	EDR on admin endpoints	Section 8.3; Exhibit G (MAL-01)	EDR coverage report	Compliant

---

Exhibit G — Security Schedule (Numbered Requirements)

The requirements in this Exhibit G are minimum requirements for the In-Scope Environment. Vendor will maintain written policies/procedures and operational controls sufficient to meet these requirements.

G1. Governance and Risk Management

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
GOV-01	Maintain a written information security program aligned to a recognized framework	ISO 27001 or NIST CSF aligned	security program overview	annual review
GOV-02	Perform documented risk assessments for in-scope systems	include threats, vulnerabilities, likelihood/impact	risk assessment summary	annual + upon material change
GOV-03	Maintain a security exception process and register	approvals + compensating controls + expiry	exception register	continuous; review quarterly
GOV-04	Maintain security awareness training	on hire + annual refresh	training completion report	annual
GOV-05	Personnel screening for Vendor Personnel with access	background checks to the extent permitted by law	screening policy + attestation	on hire; periodic where lawful

G2. Asset and Configuration Management

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
ASSET-01	Maintain inventory of in-scope assets	include cloud accounts, clusters, databases	asset inventory export	quarterly
ASSET-02	Maintain secure configuration baselines	CIS benchmarks or equivalent	baseline standard + drift report	annual + continuous monitoring
ASSET-03	Prohibit default passwords and insecure defaults	enforced at build/provision	build templates; audit results	continuous

G3. Identity and Access Management

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
IAM-01	Enforce MFA for privileged access	MFA required for all privileged accounts	MFA policy + enforcement evidence	continuous
IAM-02	Enforce MFA for production access	MFA required for production console/shell access	bastion/SSO config evidence	continuous
IAM-03	Least privilege and RBAC	roles defined; no broad admin by default	role matrix + access review	semi-annual

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
IAM-04	Deprovision access promptly	disable within 24 hours of termination	deprovision tickets/logs	continuous
IAM-05	Privileged access reviews	formal review and attestation	access review report	quarterly
IAM-06	Shared admin accounts restricted	permitted only with documented need + logging	exception register entry	continuous

G3A. Password Management (Added)

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
PASS-01	Password length/strength standard	admin 14+ chars; others 12+	password standard excerpt	annual review
PASS-02	Break-glass credential controls	vault + rotation every 90 days	vault logs + rotation record	quarterly verification
PASS-03	Brute force protections	lockout/rate limiting	configuration evidence	continuous
PASS-04	Prohibit known-compromised passwords	screening/controls	policy + tool output summary	continuous

G4. Cryptography and Secrets

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
CRYP-01	Encrypt Company Data in transit	TLS 1.2+	architecture/config evidence	continuous
CRYP-02	Encrypt Company Data at rest	AES-256 or equivalent	storage encryption evidence	continuous
CRYP-03	Key management controls	restricted access; separation of duties where feasible	KMS policy	annual review
CRYP-04	Key rotation	rotate annually or on compromise	rotation logs	annual
SECR-01	Central secrets vault	no hardcoding; access-controlled vault	vault policy + scan results	continuous

G5. Vulnerability and Patch Management

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
VULN-01	Vulnerability scanning	authenticated scanning where feasible	scan summaries	monthly
VULN-02	Penetration testing	independent test of in-scope app/env	pen test executive summary	annual
VULN-03	Patch management	risk-based patching of in-scope systems	patch compliance report	monthly
VULN-04	Remediation SLAs	Critical 7d; High 30d; Medium 60d	SLA metrics (Exhibit B)	monthly/quarterly

G6. Logging, Monitoring, Detection, and Records

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
LOG-01	Centralize logs for in-scope systems	SIEM or centralized logging	logging architecture	annual review
LOG-02	Retain logs	minimum 180 days	retention configuration	continuous
LOG-03	Monitor for material events	alerting for suspicious auth, privilege use	alert catalogue	quarterly review
LOG-04	Time synchronization	NTP or equivalent across in-scope systems	configuration evidence	continuous
REC-01	Records retention schedule	documented + enforced	schedule (Section 12.4)	annual review
REC-02	Legal hold support	preserve records when notified	procedure + attestation	per request

G7. Incident Response and Reporting

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
IR-01	Maintain incident response plan	documented + role assignments	IR plan (summary)	annual review
IR-02	Test incident response	tabletop or simulation	tabletop report	annual

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
IR-03	Notify Company of Security Incidents	within 72 hours of awareness	incident notice	per incident
IR-04	Provide incident report	RCA + corrective actions	written incident report	per incident

G8. Business Continuity and Disaster Recovery

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
BCDR-01	Maintain BC/DR plans	appropriate to Services	BC/DR plan summary	annual review
BCDR-02	Annual recovery testing	test backup restore + failover where feasible	test summary	annual
BCDR-03	Meet RPO/RTO targets	per Section 16	BC/DR results	annual + upon material change

G9. Subprocessor and Supply Chain Security

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
SUP-01	Flow-down security obligations	no less protective than this Addendum	contract excerpts	per Subprocessor
SUP-02	Subprocessor inventory	register with data categories + locations	Exhibit D	quarterly update
SUP-03	Subprocessor notice	30 days prior notice	notice records	per change

G10. Data Lifecycle Controls

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
DATA-01	Data minimization	only data needed for Services	design docs	continuous
DATA-02	Export on termination	30-day export window	export procedure	per termination
DATA-03	Deletion	delete within 60 days after export window	deletion certification	per termination

G11. Data Location (Added)

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
LOC-01	US-only hosting for Company Data	US-only for primary, DR, backups, logs	residency config evidence	continuous; review quarterly
LOC-02	Controls to prevent out-of-region storage	guardrails/policies + review	policy-as-code or config summary	quarterly
LOC-03	Location change approval	Company written consent required	approval record	per change

G12. Malware Protection (Added)

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
MAL-01	EDR/anti-malware on admin endpoints	100% coverage	coverage report	monthly
MAL-02	Malware alerting and response	documented workflow	runbook excerpt	annual review
MAL-03	Tamper protection + updates	enabled	configuration evidence	continuous

G13. Network Authentication and Authorization (Added)

ID	Requirement	Minimum Standard	Evidence/Deliverable	Frequency
NET-01	Secure admin network access	bastion/secure gateway + MFA	architecture diagram	annual review
NET-02	Network-level authentication	strong identity controls for remote admin	SSO/ZTNA config evidence	continuous
NET-03	Authorization at service layer	RBAC enforced; least privilege	role model + tests	semi-annual review

---

Exhibit H — Risk Acceptance & Remediation Plan (Template + Sample Entries)

H1. Purpose and Use

This Exhibit H documents (a) identified control gaps or deviations from Exhibit G or other requirements in this Addendum, (b) Vendor's compensating controls and remediation plan, and (c) Company's time-bound Risk Acceptance, if any. Risk Acceptance is not a waiver of Vendor's obligations; it is a conditional, temporary

accommodation subject to the terms of this Exhibit H.

H2. Workflow (Text Chart)

Step	Action	Owner	Output
1	Identify gap	Company or Vendor	finding record
2	Assess risk and scope	Vendor (with Company input)	risk rating + impact statement
3	Define compensating controls	Vendor	control description + evidence
4	Define remediation plan	Vendor	milestones + due dates
5	Approve/accept risk (if applicable)	Company	written acceptance + expiry
6	Track to closure	Vendor	status updates
7	Validate completion	Company	closure confirmation

H3. Risk Register (Sample Structure)

Risk ID	Finding / Gap	Requirement Ref	Scope	Inherent Risk	Compensating Controls	Remediation Plan & Milestones	Target Date	Risk Acceptance Expiration	Status
RA-2026-001	Break-glass on-call paging console does not support MFA	Exhibit G (IAM-01 / IAM-02 / PASS-02)	1 internal tool used by on-call SREs	Medium	Access limited to 2 named admins; IP allowlist; session logging; quarterly access review; rotate break-glass credentials every 30 days until fixed	(1) Replace console with MFA-capable tool (Mar 15, 2026). (2) Decommission legacy console (Jun 15, 2026).	Jun 15, 2026	Jun 30, 2026	Open
RA-2026-002	Network logs retained only 90 days due to vendor	Exhibit G (LOG-02 / REC-01)	VPC flow logs for non-prod	Low	Production logs retained 180 days; non-prod contains no Company Data; alerting	(1) Extend non-prod flow log retention to 180 days (Apr 30, 2026).	Apr 30, 2026	May 31, 2026	In Progress

Risk ID	Finding / Gap	Requirement Ref	Scope	Inherent Risk	Compensating Controls	Remediation Plan & Milestones	Target Date	Risk Acceptance Expiration	Status
	default				enabled				
RA-2026-003	Annual BC/DR test for identity component not completed in 2025	Exhibit G (BCDR-02 / BCDR-03)	Identity component used for admin SSO	Medium	Backups verified; failover runbook updated; monitoring tested	(1) Run tabletop failover exercise (Feb 28, 2026). (2) Execute technical failover test in staging (Mar 31, 2026). (3) Document results and remediate findings (Apr 30, 2026).	Apr 30, 2026	May 31, 2026	Open

H4. Remediation Plan Status Reporting (Semi-Structured)

Vendor will provide Company with status updates for each open Risk ID at least monthly (or more frequently for High/Critical risks), including:

Field	Example Value
Risk ID	RA-2026-001
Current status	In Progress
Last update date	February 20, 2026
Next milestone	Replace console with MFA-capable tool
Milestone due date	March 15, 2026
Blockers/Dependencies	Procurement approval; vendor migration support
Evidence available	access review report; IP allowlist policy; vault rotation log
Revised target date (if any)	none

H5. Risk Acceptance Terms

(a) **Form of Acceptance.** Any Risk Acceptance must be in writing (email acceptable) by Company's Head of Cyber Risk or delegate.

(b) **No Expansion.** Risk Acceptance applies only to the specific scope described in the Risk Register and does not extend to other systems, data, or services.

(c) **Expiration.** Each Risk Acceptance expires on the earlier of (i) completion of remediation validated by Company, (ii) the Risk Acceptance Expiration date in the Risk Register, or (iii) termination of the Agreement.

(d) **Revocation.** Company may revoke Risk Acceptance upon written notice if (i) Vendor fails to meet a milestone without reasonable justification, (ii) compensating controls are not maintained, or (iii) new information materially increases the risk.

(e) **Interim Controls.** Vendor will maintain compensating controls until remediation is complete and validated.

H6. Acknowledgement and Sign-Off

Company Approval (Risk Acceptance Authority)
Name: Alicia Gomez
Title: Head of Cyber Risk
Signature: /s/ Alicia Gomez
Date: January 15, 2026

Vendor Remediation Owner
Name: Maya Chen
Title: Director of Information Security
Signature: /s/ Maya Chen
Date: January 15, 2026

Signatures

COMPANY: Redwood Peak Financial, Inc.

By: /s/ Jordan Patel
Title: Associate General Counsel
Date: January 15, 2026

VENDOR: Nimbus Ridge Technologies, LLC

By: /s/ Maya Chen
Title: Director of Information Security
Date: January 15, 2026