

EMJ.NEXUS Security Schedule

Subscriber Reading Edition SR1 | EMJ-NEXUS-SEC-001 | v1.0

Commercial baseline 12 October 2026 | v1.0 | Subscriber edition 14 October 2026

Legal provider EMJ LIFE HOLDINGS PTE. LTD. | Singapore UEN 202445078N

Contract Effective Date is determined by the executed Order Form. Template release does not activate service.

Reading and acceptance

This document is one of the seven required Stage Two acknowledgements. At Stage Two, read and download it while completing the Enterprise profile. OF has its separate reading-and-acceptance gate after KYB and before subscription plan selection.

Complete all fourteen required profile fields and separately acknowledge MCT, DPA, SEC, SLA, DRE, EIPP and CPS. Together with cleared payment and the correct Enterprise EGC ID, these are the conditions for the once-only first 200 E-IPP Points. A document checkbox alone does not confirm payment or activate service.

1. Purpose and Scope

This Security Schedule defines the mandatory technical and organisational security commitments applicable to EMJ.NEXUS and Enterprise Data. It forms part of the EMJ.NEXUS Enterprise Contract and Governance Pack and supplements:

- EMJ.NEXUS Enterprise Subscription Master Commercial Terms;
- the applicable Enterprise Order Form;
- Data Processing Addendum;
- Service Level Agreement;
- Data Rights & Exit Schedule;
- applicable written amendments.

This Schedule applies to:

- Enterprise Input Data;
- Enterprise Personal Data;
- Evidence Objects;
- enterprise files and attachments;
- Node and Mission information;
- EGC ID information;
- E-IPP Points and E-IPP Score records;
- EMJ.NEXUS Metadata;
- JSON evidence files;
- DOI landing pages;
- encrypted download archives;
- credentials;
- security logs;
- delivery records.

EMJ.LIFE shall maintain the controls stated in this Schedule. A control may be implemented through:

- EMJ.LIFE systems;
- qualified service providers;
- Sub-processors;
- documented procedures;
- technical safeguards;
- organisational measures.

No change to security architecture, provider, technology or implementation shall materially reduce the protection required by this Schedule.

2. Security Objectives

EMJ.LIFE shall maintain controls designed and operated to protect:

2.1 Confidentiality

EMJ.LIFE shall protect Enterprise Data against unauthorised:

- access;
- disclosure;
- copying;
- use;
- alteration;
- distribution.

2.2 Integrity

EMJ.LIFE shall maintain controls to protect the:

- accuracy;
- completeness;
- provenance;
- time relationship;
- version history;
- relationship structure;
- governance status;
- delivery status;

of Enterprise Data and applicable records.

2.3 Availability

EMJ.LIFE shall maintain the Core Platform in accordance with the applicable availability commitment in the SLA. Availability is subject to:

- the SLA measurement method;
- agreed exclusions;
- maintenance;
- security controls;
- third-party dependencies;
- force majeure;
- Enterprise dependencies.

2.4 Resilience

EMJ.LIFE shall maintain operational safeguards designed to reduce the impact of:

- Security Incidents;
- system failures;
- data corruption;
- unauthorised access;
- service interruption;
- infrastructure failure;
- operational errors;
- malicious activity;
- supplier failure.

3. Security Governance

3.1 Documented minimum security baseline

EMJ.LIFE shall maintain the mandatory controls in this Schedule for activated production services and Enterprise Data, with assigned owners, documented procedures, evidence of verification, incident/corrective-action records and at least annual review.

Before activation, the responsible technical/security owner shall verify the applicable controls in the Order Form activation record. These clauses are prospective contractual commitments; their inclusion does not claim that a certification, audit, penetration test or production readiness check has already been completed. If a mandatory control is not ready, the affected service or Processing is not activated until it is implemented or a lawful equivalent-control exception is expressly agreed under Section 3.3.

3.2 Security responsibility

EMJ.LIFE shall designate personnel or functions responsible for:

- information security;
- access management;
- incident response;
- privacy coordination;
- business continuity;
- supplier and Sub-processor oversight;
- security improvement;
- security evidence.

3.3 Risk assessment and controlled exceptions

Assess security risks at least annually, before material architecture/Processing changes and after a material incident. Record control owners, severity, remediation and exception reviews.

An exception must identify the control, reason, affected scope, compensating safeguard, risk owner, expiry/review date and evidence. An exception reducing the contractual baseline requires express written agreement with the Enterprise, and may not reduce mandatory legal protection. It is not implied by a provider's technical limitation or a generic phrase such as where supported.

4. Access Control

4.1 Least privilege

Access to Enterprise Data, EMJ.NEXUS Metadata and production systems shall be limited according to:

- role;
- business need;
- least privilege;
- approved assignment;
- time limitation where appropriate.

4.2 Account management

EMJ.LIFE shall maintain procedures for:

- account creation;

- identity verification;
- role assignment;
- access approval;
- access modification;
- access review;
- suspension;
- termination;
- emergency access.

Bind a controlled invitation to the intended LEI/Enterprise and designated mailbox; verify mailbox control, enforce the invitation/account scope and record approval or failure. A forwarded invitation does not automatically authorise another mailbox or entity. Changes to the mailbox/entity association require controlled review and an attributable authoriser; these checks do not replace signatory or privileged-access authority.

4.3 Authentication

Privileged production, cloud-console and Enterprise administrator access shall require multi-factor authentication, unique accounts and controlled session/credential practices. Standard user authentication shall use verified identity/contact, secure credentials or an approved federated method, with brute-force protections and secure credential reset.

SSO, device/network restrictions or customer-specific methods are included only when expressly supported in the Order Form. A lawfully approved equivalent control must follow Section 3.3. Shared ordinary administrator credentials are prohibited; logged, time-limited emergency access is separately controlled.

4.4 Privileged access

Privileged access is approved individually, limited to necessary duties, protected by MFA, recorded in tamper-resistant access/change logs and reviewed at least quarterly. Revoke access promptly upon termination or loss of role; emergency privileges are time-limited and reviewed after use. Development/test personnel have no automatic production-data access.

4.5 Enterprise responsibilities

The Enterprise shall:

- manage its users;
- protect credentials;
- use approved authentication methods;
- prevent credential sharing;
- report suspected compromise promptly;
- remove access when a user changes role or leaves;
- maintain appropriate internal access reviews.

5. Data Protection Measures

5.1 Data classification

EMJ.LIFE shall maintain a classification approach distinguishing, where applicable:

- public information;
- internal information;
- confidential information;

- restricted information;
- Personal Data;
- sensitive or regulated information;
- security and credential information.

5.2 Data minimisation

EMJ.LIFE shall support data minimisation through:

- limited required fields;
- controlled file submission;
- restricted access;
- retention rules;
- deletion or anonymisation processes;
- data-scope controls.

The Enterprise remains responsible for not submitting unnecessary, excessive or unlawful data.

5.3 Tenant separation

EMJ.LIFE shall maintain controls designed to prevent unauthorised access between:

- Enterprises;
- users;
- roles;
- workspaces;
- environments;
- delivery packages.

5.4 Metadata separation

EMJ.NEXUS Metadata may support platform-wide technical and governance functions. EMJ.LIFE shall not disclose one Enterprise's confidential Enterprise Data to another Enterprise merely because common platform Metadata exists.

5.5 Logging and review

Maintain protected records of authentication, privileged administration, material data access, security events, configuration changes, governance-state transitions, delivery, export and deletion. Log the actor or authorised service, timestamp, relevant object and outcome where applicable; restrict access and detect unauthorised alteration.

Identifiable operational/security logs use the DRE Section 14 retention schedule, ordinarily no more than 180 calendar days rolling unless a documented lawful need applies. Logs must not retain unnecessary evidence payloads, plaintext credentials or encryption keys. Review material security alerts promptly under the incident-response process; lawful deletion obligations apply to identifiable log content.

Record LEI source values/query dates, source-gap resolutions, invitation verification, payment confirmation, EGC ID issuance, PROFILE_COMPLETE, each of the seven Stage Two document acknowledgements, first allocation and current task restriction/restoration as separate protected events. Preserve the original and later source versions; ordinary Enterprise profile editing shall not overwrite the authoritative snapshot. Retain tax and contact data only within the DPA purposes and schedules.

Enforce once-only EGC ID association and initial allocation through entity/identifier consistency and duplicate-safe payment/allocation handling. Repeated provider notifications, profile submissions or optional D-U-N-S enrichment must not create

repeated grants. Correct demonstrable errors with the prior state retained, rather than silently changing a balance.

6. Encryption and Key Management

6.1 Encryption in transit

Protect Enterprise Data crossing public or untrusted networks with TLS 1.2 or later, or a comparably secure current transport method approved under Section 3.3. Disable known insecure legacy protocols for contracted production endpoints. Verify certificates and protect administrative and export channels.

6.2 Encryption at rest

Encrypt Enterprise Data in production storage, backups and delivered archives using AES-256 or a comparably strong current method. Passwords are stored as appropriately salted one-way hashes rather than reversible plaintext. Restrict key access separately from ordinary data access and use controlled key custody.

Any system requiring an equivalent alternative must have the specific prior exception under Section 3.3. Unencrypted storage is not automatically permitted because a supplier lacks the feature.

6.3 Key management

EMJ.LIFE shall maintain controls for:

- key generation;
- key storage;
- key access;
- key rotation;
- key backup;
- key revocation;
- key destruction;
- separation of key-management duties.

6.4 Encrypted download archives

For encrypted download archives:

- EMJ.LIFE shall provide the agreed archive format;
- the Enterprise shall control internal key custody after delivery;
- the Enterprise shall protect download links, credentials and keys;
- EMJ.LIFE shall maintain delivery and archive records;
- compromise caused by the Enterprise's failure to protect delivered credentials or keys remains the Enterprise's responsibility.

7. Secure Development and Change Management

7.1 Secure development

EMJ.LIFE shall maintain secure-development practices, including where proportionate:

- security requirements;
- code review;
- dependency management;
- vulnerability testing;
- separation of development, test and production;
- restricted production access;

- secure configuration;
- release approval;
- remediation tracking.

7.2 Change management

Material production changes shall be:

- authorised;
- assessed for security impact;
- tested where appropriate;
- documented;
- implemented through controlled procedures;
- capable of rollback where reasonably practicable.

7.3 Emergency changes

EMJ.LIFE may implement emergency changes without the full standard process where necessary to:

- address an active security threat;
- restore service;
- comply with law;
- protect Enterprise Data;
- prevent material harm.

Emergency changes shall be documented and reviewed after implementation.

8. Vulnerability and Security Testing

8.1 Vulnerability management and remediation

Maintain asset/dependency inventories, risk-ranked vulnerability tracking and remediation verification. Assess an actively exploited critical issue promptly and apply containment or effective mitigation within twenty-four hours after validation where within EMJ.LIFE's control. Default remediation targets after validation are seven calendar days for critical, thirty for high and ninety for medium severity.

If a supplier fix is unavailable or full repair is impracticable, implement effective compensating protection, record the reason and revised plan, notify an affected Enterprise of material risk and use the Section 3.3 exception process. A target extension does not excuse a failure to maintain mandatory protection or incident notice.

8.2 Security and recovery testing

Conduct vulnerability/configuration scanning at least monthly and after material production changes. Conduct an independent or appropriately separated penetration/security assessment at least annually and before a materially changed high-risk public component is first activated. Verify tenant access separation and remediate tracked material findings.

Test representative backup restoration at least quarterly and the material incident/continuity procedure at least annually. Keep scope, date, results and corrective-action evidence. No assessment report or certificate is claimed to exist until it is actually recorded and available under Section 18.

8.3 Enterprise testing

The Enterprise shall not conduct security testing, scanning, penetration testing or denial-of- service testing against EMJ.NEXUS without EMJ.LIFE's prior written approval. Approved testing shall:

- have a defined scope;
- avoid unnecessary disruption;
- protect other customers;
- comply with testing rules;
- preserve confidentiality;
- provide results to EMJ.LIFE where reasonably required.

9. Incident Response

9.1 Incident response programme

EMJ.LIFE shall maintain procedures for:

- incident identification;
- triage;
- severity classification;
- containment;
- eradication;
- recovery;
- evidence preservation;
- notification;
- post-incident review;
- corrective action.

9.2 Security Incident notification

Notify the affected Enterprise without undue delay after becoming aware of a material Security Incident or credible indications of one affecting its service/data confidentiality, integrity or availability. Initial information may be preliminary and shall include available scope, known/suspected impact, containment, recovery, recommended actions, relevant times and contact.

Continue material updates as information becomes available. A Personal Data Breach additionally follows the DPA's awareness/credible-grounds trigger, irrespective of the operational severity label or Support Hours. Final confirmation and completion of an investigation are not prerequisites to legally required notice.

9.3 Personal Data Breach

A Personal Data Breach is governed by the DPA. If an event is both a Security Incident and a Personal Data Breach, the notification and cooperation obligations of both documents apply.

9.4 Incident cooperation

The Enterprise shall:

- provide reasonable information;
- cooperate in containment;
- preserve relevant logs and evidence;
- follow reasonable security instructions;
- identify affected Enterprise users where necessary;
- avoid interfering with the investigation.

10. Business Continuity and Disaster Recovery

10.1 Continuity planning

EMJ.LIFE shall maintain continuity procedures covering:

- critical service functions;
- key personnel;
- infrastructure failure;
- supplier failure;
- Security Incidents;
- data corruption;
- communications;
- recovery priorities.

10.2 Backup baseline

Maintain encrypted backups of contracted core evidence and configuration data at least daily, with access separation, integrity checks, documented recovery procedures and an ordinarily thirty-calendar-day rolling backup window. Record actual systems, location, frequency and any agreed enhancement in DPA Annex A and the activation record.

The maximum delayed deletion cycle for isolated backup copies is ninety calendar days after the corresponding production deletion, subject to any earlier legal requirement. Restoration reapplies deletion and access restrictions before ordinary use. Backup frequency is a design obligation, not a guaranteed RTO, RPO or zero-loss warranty; specific recovery guarantees require an express SLA/Order Form commitment.

10.3 Recovery testing

Test representative restore procedures at least quarterly, documenting scope, successful/unsuccessful outcomes and corrective actions. Retest a materially failed restore after correction. The annual continuity exercise and supplier failure plan are covered by Section 8.2. An actual failure or threat is managed under Sections 9 and 10.1 and the SLA.

10.4 SLA relationship

Specific RTO, RPO, availability and Service Credit commitments apply only as expressly stated in the SLA or Order Form. Backups do not guarantee that every item can be restored or that restoration will occur within a specific period unless expressly agreed.

11. Physical and Environmental Security

To the extent EMJ.LIFE or its providers control relevant facilities, EMJ.LIFE shall maintain reasonable measures addressing:

- facility access;
- visitor management;
- environmental risks;
- power and connectivity;
- equipment protection;
- media handling;
- secure disposal;
- physical monitoring.

Where infrastructure is hosted by a third-party provider, EMJ.LIFE shall maintain supplier due- diligence and contractual controls appropriate to the service and risk.

12. Personnel Security

EMJ.LIFE shall maintain personnel controls, including where appropriate:

- role-based screening;
- confidentiality agreements;
- security awareness;
- privacy training;
- acceptable-use requirements;
- access restrictions;
- disciplinary procedures;
- offboarding;
- return or removal of credentials and assets.

Personnel with access to Enterprise Data shall receive guidance appropriate to their responsibilities.

13. Sub-processor and Supplier Security

EMJ.LIFE shall:

- assess relevant security risks of material Sub-processors;
- impose security and confidentiality obligations;
- limit Sub-processor access;
- monitor material security performance where appropriate;
- manage Sub-processor changes under the DPA;
- address material supplier incidents;
- maintain appropriate supplier records.

EMJ.LIFE remains responsible for Sub-processor obligations to the extent stated in the DPA and applicable law.

14. Data Retention, Deletion and Media Disposal

14.1 Retention controls

EMJ.LIFE shall maintain controls to:

- identify retention requirements;
- apply deletion or anonymisation schedules;
- restrict retained data;
- preserve legal holds;
- avoid unnecessary retention;
- document deletion or retention exceptions.

14.2 Secure deletion and permitted retention

Apply DRE Section 14 and DPA Sections 17/23 to production deletion, isolated backups, lawful holds and confirmations. An archive, Metadata/IP label, technical recovery preference or historical-version requirement does not override a mandatory deletion duty. Retained copies require documented lawful purpose, limited access and a review/end date; expired holds and unnecessary personal information are deleted or irreversibly anonymised.

14.3 Media disposal

Storage media and equipment containing Enterprise Data shall be securely erased, destroyed or otherwise rendered inaccessible before disposal or reuse where technically and commercially practicable.

15. Security of DOI, JSON and Compendium Deliverables

15.1 JSON evidence files

EMJ.LIFE shall maintain controls to protect:

- JSON evidence files;
- manifests;
- version records;
- integrity information;
- delivery records.

15.2 DOI metadata and evidence-file access

Separate the DOI's minimum registration/landing metadata from its evidence payload. Registration metadata may be public and obtainable through the registration agency, even where files are Private. Only the approved minimum non-confidential metadata is registered; necessary publication consent and restrictions are recorded under CPS Section 10.

Private evidence payload is available only to authorised Enterprise/provider users. Controlled Access permits approved named recipients; public payload release requires express written scope/consent and permissions. A DOI does not authorise public release of confidential files, personal information or archive keys.

15.3 Encrypted archives

EMJ.LIFE shall provide encrypted archives according to the applicable Compendium Schedule or Order Form. The Enterprise shall protect:

- secure receipt;
- internal access;
- key custody;
- storage;
- backup;
- authorised distribution;
- prevention of unauthorised public disclosure.

15.4 Delivery records

EMJ.LIFE may retain:

- delivery date;
- recipient;
- download record;
- file version;
- checksum or integrity information;
- re-delivery record;
- withdrawal or supersession record.

16. Evidence Integrity and Governance Controls

Preserve source, event/record timestamps, versions, relationships, rights, state transitions, authorised delivery and correction history, using attributable, append-only state records where lawful. Record original and corrected versions with changed-by, authority, reason and effective date; do not silently overwrite a prior relevant state.

State domains are distinct: publication/evidence state (ACTIVE, SUPERSEDED, HISTORICAL, WITHDRAWN); service activation (SCHEDULED, NOT_ACTIVE, ACTIVE);

governance review (ELIGIBLE_FOR_REVIEW, UNDER_REVIEW, HOLD, ESCALATED); account access (Active, Suspended, Restricted, Inactive); and payload access (Private, Controlled Access, Public). A status in one domain is not an implicit status in another.

Historical preservation is subject to the DPA and lawful deletion, with minimal non-identifying event markers where appropriate. Integrity controls do not transform a platform record into audit, assurance, certification, legal proof or regulatory approval.

Additional independent domains are LEI reference status (EntityStatus and RegistrationStatus separately), controlled invitation verification, subscription eligibility, payment, EGC ID issuance, profile completeness, Point allocation and task/new-evidence permissions. PROFILE_COMPLETE does not mean external verification; EntityStatus ACTIVE is not a platform publication status; LAPSED is not company closure. Current source refresh and a recorded restriction do not silently invalidate lawful historical events.

Implement MCT Section 5.7 task gates, the disclosed OF Section 5.4 refresh/failure configuration, reasoned notices and review/restoration. A failed query is an unknown/freshness event, not a fabricated source-state change. Restrict only affected new activity; preserve lawful profile correction, history and export. Security/system faults in these controls remain subject to this Schedule and the SLA, not blanket third-party exclusion.

17. Enterprise Security Responsibilities

The Enterprise shall:

- protect credentials and authentication devices;
- use strong access controls;
- limit user permissions;
- prevent credential sharing;
- review user access;
- report suspected compromise promptly;
- submit only lawful and necessary data;
- maintain endpoint and network security;
- protect delivered files and encryption keys;
- maintain backups of data it must retain;
- ensure integrations meet security requirements;
- follow EMJ.LIFE security instructions;
- ensure third-party users and Nodes comply with applicable obligations.

EMJ.LIFE is not responsible for an incident caused primarily by:

- compromised Enterprise credentials;
- unauthorised Enterprise configurations;
- unsupported software;
- insecure Enterprise integrations;
- failure to follow required security instructions;
- unauthorised disclosure by the Enterprise;
- loss of delivered encryption keys.

18. Security information and assurance boundaries

Provide information reasonably necessary to demonstrate the contracted security controls, subject to confidentiality, protection of other customers and proportionate safe disclosure. This may include policy/control summaries, actual assessment scope/date, remediation summaries, approved exceptions and questionnaire

responses. Where an existing independent report sufficiently answers a request it may be supplied instead of duplicate testing.

No ISO, SOC, penetration-test completion or equivalent certification is represented unless specifically identified with its issuer, scope, date and current status in an authorised written record. No source code, keys, exploitable details or other-customer data is required where a suitable safe demonstration provides the necessary assurance. DPA audit rights and mandatory law remain unaffected.

19. Security Incident and Data-Protection Relationship

This Security Schedule shall be read with the DPA. The DPA governs:

- Personal Data Processing;
- Data Subject rights;
- Personal Data Breaches;
- cross-border data transfers;
- Sub-processor Processing obligations;
- data-protection cooperation.

This Schedule governs:

- technical security;
- organisational security;
- access control;
- encryption;
- incident response;
- continuity;
- infrastructure and operational safeguards.

Where the same event is covered by both documents, both sets of obligations apply.

20. Termination and Exit Security

Upon termination or expiry, EMJ.LIFE shall apply controls to:

- restrict former users;
- deactivate or restrict credentials;
- preserve authorised Historical Records;
- support data export;
- protect export files;
- delete or anonymise data as required;
- maintain legal-retention controls;
- prevent unauthorised post-termination access;
- document material deletion or retention exceptions.

The Enterprise shall:

- export required data within the applicable exit period;
- protect received files;
- revoke former personnel access;
- return or delete EMJ.LIFE credentials;
- protect encryption keys;
- cease using Restricted or Inactive EGC IDs for new activity.

21. Audit and Review

EMJ.LIFE shall periodically review this Schedule and related security measures. The review shall consider:

- incidents;
- vulnerabilities;
- architecture changes;
- regulatory requirements;
- customer risk;
- Sub-processor changes;
- audit findings;
- recovery testing;
- technology changes;
- control exceptions.

The Enterprise may exercise audit rights according to the DPA and the Agreement.

22. Security Commitment Boundary

EMJ.LIFE is accountable for its contracted controls, provider-selected infrastructure/Sub-processor oversight, incident handling and actual verification before activation. A third-party supplier relationship does not by itself excuse those duties.

The Enterprise remains responsible for its own devices/networks, credentials, permissions, instructions, independently chosen integrations, lawful data and delivered-file/key custody. No party guarantees the absence of every threat or external regulatory/assurance outcome. Liability and direct remedies remain governed by the MCT, DPA and SLA, rather than blanket removal of provider responsibility for all third-party failures.

23. Term and Survival

This Schedule begins when the applicable Enterprise Contract and Governance Pack becomes effective and continues while EMJ.LIFE provides EMJ.NEXUS or retains Enterprise Data. The following obligations survive for as long as relevant:

- confidentiality;
- access restriction;
- data protection;
- secure retention;
- incident cooperation;
- legal preservation;
- deletion and anonymisation;
- Historical Records protection;
- security of delivered files;
- restrictions on post-termination access.

24. Incorporation and Execution

This document is incorporated into the Agreement by the executed Enterprise Order Form identifying its controlled document ID, v1.0, issue date 12 October 2026 and subscriber release SR-20261014-01 based on CP-20261012-R03. The supplied release register identifies the applicable file fingerprints. Separate signatures on this document are not required, except the parties execute the Order Form by signature or recorded electronic acceptance under MCT Section 25.7. Party identity, both parties' authorised acceptance and the Contract Effective Date are recorded in the Order acceptance receipt. Annexes and express amendments are effective only under MCT Section 24; this template revision does not automatically amend an earlier executed Agreement.

Subscriber acknowledgement

☐ I have read and agree to the Security Schedule and the disclosed security scope, controls and verification requirements.

This acknowledgement is recorded during Stage Two, separately from OF. Its document ID, version, Subscriber account, exact accepted version and actual time are linked to the Enterprise and EGC ID. All seven document acknowledgements and all fourteen required fields must be complete before the first 200 E-IPP Points are allocated. No separate signature or repeated corporate questionnaire is required for this document.

Stage Two completion and initial Points

All fourteen required fields in MCT Section 5.5 must be complete. D-U-N-S is the fifteenth, optional field. A permitted source-gap or tax-not-applicable resolution must be documented; unresolved or fabricated values do not satisfy a required field.

The first 200 E-IPP Points are allocated once only when cleared subscription payment, the correct Enterprise EGC ID, completion of all fourteen required profile fields, and the seven separate Stage Two document acknowledgements are recorded for the same Enterprise. The seven documents are MCT, DPA, SEC, SLA, DRE, EIPP and CPS.

Acceptance of OF alone does not satisfy this gate. D-U-N-S is optional and is excluded from the required-field and document checks.

The fourteen-field completion result and each of the seven document acknowledgements are recorded separately and linked to the same Enterprise. All must be complete, with cleared payment and EGC ID, before the once-only initial allocation. OF acceptance does not substitute for the seven acknowledgements. Point usability and service/task activation remain governed by their separate conditions.