

EMJ.NEXUS Enterprise Digital Behaviour Evidence Compendium Schedule

Subscriber Reading Edition SR1 | EMJ-NEXUS-CPS-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 Schedule establishes the mandatory rules for the optional, one-time Enterprise Digital Behaviour Evidence Compendium service provided through EMJ.NEXUS. It governs:

- eligibility;
- application;
- evidence continuity;
- fees and payment;
- production instructions;
- review and acceptance;
- delivery;
- JSON evidence files;
- DOI landing pages;
- encrypted download archives;
- manifests;
- integrity information;
- versioning;
- corrections;
- supersession;
- access status;
- publication restrictions;
- cancellation;
- delay;
- rejection;
- third-party permissions;
- privacy;
- post-termination treatment.

This Schedule 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;
- Security Schedule;

- Service Level Agreement;
- Data Rights & Exit Schedule;
- E-IPP Points & Score Policy;
- applicable written amendments.

This Schedule governs Compendium-specific matters. It does not replace:

- the DPA for Personal Data Processing;
- the Security Schedule for security controls;
- the SLA for platform availability and support;
- the Data Rights & Exit Schedule for ownership, export and exit;
- the E-IPP Policy for Points and Score;
- the Master Commercial Terms for general commercial terms, liability, confidentiality and dispute resolution.

2. Definitions

2.1 Enterprise Digital Behaviour Evidence Compendium

“Compendium” means a controlled evidence deliverable prepared through EMJ.NEXUS that organises eligible Enterprise digital-behaviour evidence and associated governance information for a defined evidence period. The accepted production scope determines which of the following content categories apply. Section 8 specifies the mandatory core deliverables:

- Enterprise-submitted evidence;
- Evidence Objects;
- source and provenance information;
- time and continuity information;
- version information;
- relationship information;
- Node and Mission relationships;
- governance and status Metadata;
- integrity information;
- delivery information;
- a JSON evidence file;
- a DOI landing page;
- an encrypted download archive;
- a manifest;
- a version or limitation statement.

2.2 Compendium is a controlled deliverable

A Compendium is a controlled evidence and governance deliverable. It is not automatically:

- an audit;
- a review;
- an assurance engagement;
- a verification;
- a certification;
- a legal opinion;
- a regulatory filing;
- a sustainability report;
- an ESG rating;
- a carbon credit;
- a carbon reduction;

- a performance guarantee;
- a compliance determination;
- a supplier qualification;
- an investment or financing document.

3. One-Time Service

3.1 One-time production and publication-record duties

Each accepted Compendium request buys one production/delivery service and does not renew automatically, regenerate later evidence, create a future-year entitlement or include ongoing interactive platform access.

After registration, the minimum DOI resolving publication/status record is maintained while EMJ.LIFE remains its responsible publisher under Section 10. This limited publication-identity duty is separate from perpetual hosting of confidential payload, which is not included. Enterprise retention/use of delivered files survives under DRE Section 4.2; download availability and deletion follow the DRE/DPA.

3.2 Separate application

The Enterprise shall submit a separate application for each Compendium. The application shall identify:

- requested Compendium name;
- Enterprise legal entity;
- EGC ID;
- evidence period;
- applicable Mission or scope;
- Nodes or relationships to be included;
- requested access status;
- delivery contact;
- publication instruction;
- required exclusions, redactions or restrictions.

4. Eligibility Requirements

4.1 Minimum eligible evidence period

A standard Compendium requires at least 180 consecutive calendar days of eligible governed evidence associated with the correct Enterprise/EGC ID and supported by attributable source, time, rights, version and relationship records. The requested period must lie within an active eligible Subscription and be sufficiently substantiated for the requested scope.

This does not require a task claim or upload every day. It requires evidence capable of supporting the defined continuous period and its limitations. Reaching day 180 does not automatically create a DOI or a production entitlement; separate application, lawful permissions, review and payment are required. Task reissuance controls are distinct from evidence-period duration.

Paid EGC ID issuance does not itself begin 180 days of eligible governed evidence. New task/evidence activity must satisfy the profile and current permissions in MCT Sections 5.5 to 5.7. Confirm the requested period from actual eligible records; neither the profile-completion date, initial 200 allocation nor payment manufactures daily participation or retroactive evidence. Historical requests already lawfully accepted remain governed by Section 20.

4.2 Continuity interruptions and incident assessment

Actual termination/expiry/non-renewal, an unsubstantiated material gap, unlawful backdating, unresolved identity/rights conflict or a material integrity failure may make the period ineligible. Document the actual reason and affected period.

Temporary protective suspension, a provider technical outage, an uneventful day or a pending review does not automatically invalidate all continuity. Apply DRE Section 9.1 to original timely source records, event time, preserved relationships and recoverability; record any genuine gap or limitation. A provider-caused incident is not automatically labelled an Enterprise breach.

Reactivation cannot fabricate activity in an inactive gap. Late authorised recovery must identify original event time separately from ingestion/recovery time and may not silently erase a real interruption.

A LEI LAPSED/EntityStatus or profile hold restricts the affected new activity under MCT Section 5.7 but does not automatically invalidate earlier lawful evidence, registered DOI identity or an already accepted production request. Preserve source-query status and the actual affected interval, assess real continuity/rights limitations under this section and DRE Section 9, and use the Section 7.2 reasoned pause/remedy only where production is actually prevented.

4.3 Confirmed production period

The application states the requested start/end dates and scope. Before accepting payment for production, EMJ.LIFE confirms the eligible period and any limitations in writing. A standard request must contain a substantiated uninterrupted qualifying period of at least 180 calendar days.

A shorter or interrupted historical dataset may be exported or separately scoped as a limited historical deliverable, but shall not be represented as a standard eligible 180-day Compendium. Two periods divided by an inactive gap are not silently merged to meet the threshold.

5. Compendium Application

5.1 Required information

The Enterprise shall provide:

- legal entity name;
- EGC ID;
- authorised applicant;
- requested title;
- evidence period;
- Mission scope;
- Node scope;
- requested DOI status;
- distribution scope;
- required redactions;
- data-source permissions;
- contact details;
- complete production instructions.

5.2 Authorised applicant

The applicant shall be:

- an authorised Enterprise representative;
- an authorised administrator;
- an approved legal or compliance contact;
- another person accepted by EMJ.LIFE.

EMJ.LIFE may verify the applicant's authority before processing the application.

5.3 Complete application and timely eligibility decision

The application is complete when legal entity/EGC ID, authorised applicant, requested period/title, task/Node scope, source material, data rights, intended recipients, metadata/payload publication consents, redactions, delivery contact and production instructions are provided.

Within two Business Days of receipt, identify genuinely missing information. Within five Business Days after complete information is supplied, confirm eligibility/approved scope or give a reasoned rejection. Provider-held records shall not be treated as an unresolved customer requirement. Payment is requested for an approved request; it is a production prerequisite, not a substitute for eligibility review.

6. Fee and Payment

6.1 Compendium fee

The standard fee is USD 1,000 per one-time Compendium, exclusive of applicable taxes, payable before production. It is separate from the annual Subscription Fee and includes all seven core deliverables in Section 8.

Additional formats or bespoke work are charged only if separately disclosed and accepted. Customer convenience cancellation after production begins is ordinarily non-refundable, but this does not exclude provider-default, non-delivery, production-error or mandatory-law remedies under Sections 7, 16 and 18.

6.2 Taxes

The Enterprise is responsible for applicable:

- GST;
 - VAT;
 - sales tax;
 - withholding tax;
 - digital-services tax;
 - duties;
 - similar government charges;
- except taxes imposed on EMJ.LIFE's net income.

6.3 Payment prerequisite

Payment clearance means cleared funds or confirmed settlement through the agreed payment provider. An alternative credit arrangement must be expressly accepted in writing with due date and scope; a purchase order alone is not cleared payment.

Where an accepted credit arrangement expressly permits production before receipt of funds, the payment prerequisite is met on that arrangement's effective date. Record that distinction in the production notice rather than describing an unpaid purchase order as settled cash.

6.4 Production eligibility

Production requires a confirmed eligible period and approved scope, complete instructions/materials, required rights and consents, completed privacy/security review, and cleared payment or an express effective production-credit arrangement. Payment alone guarantees neither eligibility nor permission to publish. Section 7.3 fixes the start date once those objectively identified conditions are complete.

7. Production and Delivery

7.1 Binding seven-calendar-day delivery

EMJ.LIFE shall deliver all core deliverables within seven calendar days after the Production Start Date, subject only to the recorded customer/legal pause and external-registration long-stop remedy in Section 7.2. Delivery includes accessible agreed files, a registered DOI and its resolving approved metadata record, required access controls, archive/key instructions, manifest and version/integrity/delivery records.

Third-party search indexing is not a deliverable or prerequisite and does not pause this period. EMJ.LIFE's own routine staffing, avoidable processing delay or incomplete internal workflow does not postpone a confirmed start date.

7.2 Defined pauses and external-registration delay

If a genuinely missing customer permission/material, a customer-requested scope change or a binding legal/security restriction prevents production, promptly give written notice identifying the affected work, reason, start time, information/actions needed and expected next review. Pause only the affected work and only for its actual necessary duration; confirm resumption. Do not impose an unrecorded or indefinite pause.

If the DOI registration agency is delayed, notify the Enterprise before the seven-day deadline, supply any safe completed files and available status record, and propose a time-bounded extension. A pending DOI/status record is not full delivery unless the Enterprise expressly accepts a revised scope. No extension for third-party indexing is permitted.

If full delivery is not achieved within fourteen additional calendar days after the original due date, excluding a documented Enterprise-caused lawful pause, the Enterprise may choose cancellation and a full Compendium fee refund within thirty calendar days, or expressly agree a revised delivery date or accepted partial scope with an agreed fee adjustment. A customer is not forced to accept only credit. Earlier material-breach and mandatory rights remain unaffected; MCT force majeure does not remove this express undelivered-fee remedy.

7.3 Production Start Date and confirmation

The Production Start Date is the calendar date when the last objectively required item in Section 6.4 is complete. EMJ.LIFE shall confirm that date and the seven-calendar-day due date in writing within two Business Days. Failure to issue the notice does not indefinitely postpone a start whose prerequisites are demonstrably complete.

The notice states the approved period/scope, core files, public metadata consent, payload access, payment basis, named recipient and any expressly accepted extension. Subsequent scope changes require recorded agreement; they do not silently replace the original due date.

8. Mandatory core deliverables

Core deliverable	Included standard requirement
JSON evidence file	Yes; Section 9 content and attributable scope/status
Registered DOI and metadata landing record	Yes; minimum approved public identity, with payload access controlled separately
Encrypted download archive	Yes; agreed files and secure key/receipt instructions
Manifest	Yes; file names, sizes, versions and relationships
Version record	Yes; identifier, issue time, approved period and correction relationships
Integrity information	Yes; SHA-256 or agreed comparable checksums and validation instructions
Delivery record	Yes; recipient, time, package/version and access status
Limitation/status statement	Included whenever limitations or restrictions apply

These core items are not optional Yes/No elections. Additional PDF, XBRL, XLSX or another custom format is included only if expressly approved, technically supported and listed in the accepted request with any separate fee. No requirement of outside audit, assurance or search-engine indexing is implied.

9. JSON Evidence File

9.1 Required contents

The JSON evidence file shall include, where applicable:

- Compendium identifier;
- Enterprise identifier;
- EGC ID;
- evidence-period information;
- Evidence Object identifiers;
- source information;
- timestamps;
- version information;
- relationship information;
- Node and Mission associations;
- status fields;
- integrity information;
- delivery information;
- applicable limitation statements.

Where enterprise identity/profile information is included, identify the LEI and internal EGC ID separately; distinguish source snapshot/date from current status, enterprise operating supplements and derived SICS classification/version. Include private tax/contact information or optional D-U-N-S matching material only where necessary, permitted and within the expressly approved recipient/publication scope.

PROFILE_COMPLETE or MATCHED is not an audit, certification or external-compliance conclusion.

9.2 Delivered-file rights and schema ownership

The Enterprise may retain and use lawfully delivered JSON and its embedded enterprise-specific descriptive Metadata for accurate internal and authorised external evidence purposes under the surviving licence in DRE Section 4.2. Subscription expiry does not revoke that right merely because platform access ends.

EMJ.LIFE/licensors retain platform schema, data model, proprietary implementation, governance and scoring logic. The Enterprise may not operate a competing infrastructure from those proprietary models or exceed licensed-content permissions. Clearly labelled internal working/derivative copies are allowed; they must not be represented as original issued files. Personal Data, confidentiality, third-party rights, limitation statements and lawful correction/withdrawal restrictions continue to apply.

9.3 File integrity

The Enterprise shall not:

- modify the JSON file and represent it as the original issued file;
- remove version information;
- remove DOI information;
- remove delivery information;
- remove integrity information;
- remove limitation statements;
- represent an amended copy as an original EMJ.LIFE deliverable.

The Enterprise may create an internal derivative or working copy if it clearly identifies the derivative status.

10. DOI Landing Page

10.1 Registration metadata and evidence-payload access

A registered DOI establishes publication identity, not confidentiality or verification. Separate the minimum registration/landing metadata from the evidence payload. With agencies such as Crossref, submitted registration metadata can be public through APIs and discovery services even if downloadable files are Private.

Before registration, obtain express written approval of the specific minimum public fields: DOI/record ID, non-confidential title, publisher, publication date, version, lawful enterprise identity where approved, period/description to the approved extent, resolving URL and status/rights boundary. Avoid personal names, source payload, sensitive Node details or confidential business information unless necessary and lawfully approved. The application records agency and approved metadata fields.

If the Enterprise cannot approve necessary public metadata, do not register a DOI or present the result as a registered Compendium. Agree a separately described non-DOI evidence export or reject/refund the unproduced request. Public metadata approval does not approve public payload release.

10.2 Private payload

Private means the confidential evidence payload is accessible only to authorised Enterprise and EMJ.LIFE users through controls. It does not mean an agency-registered DOI or its approved minimum metadata is invisible. Public minimal resolution/status may remain while payload files are protected. Archive keys and private source material are never published merely because a DOI exists.

10.3 Controlled Access payload

Controlled Access permits only verified recipients authorised by the Enterprise and accepted within applicable rights, such as advisers, auditors, customers or regulators. Record recipient/role, scope, access duration and onward-disclosure restrictions. It is not unrestricted public access. The minimum public DOI metadata remains separate.

10.4 Public payload by express written consent

Public release of evidence files or substantive landing content requires separate express written approval of the publication scope, necessary Personal Data/legal basis, third-party/licensed-content rights and redactions. EMJ.LIFE verifies the publication configuration before release.

Publishing the DOI metadata alone does not release the payload. A later access change has an attributable authoriser, reason, effective time and status history; it cannot retroactively remove recipients' previously lawful access or mandatory rights.

10.5 DOI limits and publication continuity

A DOI does not prove external verification, assurance, certification, legal compliance, regulatory approval or institutional endorsement. Third-party indexing and acceptance are outside EMJ.LIFE's control and are not part of the seven-day delivery commitment.

While EMJ.LIFE remains the responsible publisher, retain the lawful minimum resolving publication/status record and version relationships; Subscription end does not silently erase a registered identity. Confidential payload hosting/download is not perpetual and follows DRE exit/retention rules. Registration metadata may remain public after withdrawal or payload deletion. Lawful withdrawal/redaction and a business-continuity successor are documented with minimum lawful status under DRE Section 18.

11. Encrypted Download Archive

11.1 Encrypted archive delivery

Every standard Compendium includes an encrypted archive containing the agreed JSON, authorised included evidence material, manifest, version/integrity/delivery information and any limitation statement. Use the Security Schedule's encryption/key controls and provide verification/download instructions to the approved recipient.

Download access remains available during the active applicable service and the 180-day Exit Period, subject to lawful security restrictions and deletion instructions. The Enterprise retains downloaded copies under DRE Section 4.2 and is responsible for its own lawful preservation/key custody.

11.2 Enterprise responsibilities

After delivery, the Enterprise shall be responsible for:

- secure receipt;
- download;
- key management;
- internal storage;
- backup;
- access control;
- authorised distribution;
- prevention of unauthorised decryption;
- prevention of public disclosure;
- retention under its own obligations.

11.3 Key loss

EMJ.LIFE is not responsible for inability to access an archive caused by:

- lost keys;
- compromised credentials;
- unauthorised deletion;
- internal access restrictions;
- failure to download during the available period;
- failure to maintain an approved recovery process.

Additional re-delivery or archive reconstruction may be subject to a reasonable fee.

12. Manifest and Integrity Information

12.1 Manifest

Include file name, size, version, package identifier, production/export date, applicable relationship, access/status boundary and checksum for each delivered core file. Identify excluded attachments and any permitted additional format so scope is verifiable. Checksum protection demonstrates file integrity, not the truth or legal sufficiency of the underlying submitted evidence.

12.2 Integrity information

Integrity information shall support:

- file verification;
- version control;
- delivery tracking;
- detection of unauthorised alteration;
- historical continuity;
- controlled reproduction.

Integrity information does not constitute:

- an external assurance conclusion;
- a certification;
- legal authentication in every jurisdiction;
- a guarantee that the underlying Enterprise Data is truthful;
- a guarantee of third-party acceptance.

13. Enterprise Data and Third-Party Rights

13.1 Enterprise responsibilities

The Enterprise shall be responsible for:

- legality of submitted data;
- data accuracy;
- evidence authenticity;
- source permissions;
- Node permissions;
- Mission permissions;
- Personal Data notices;
- third-party rights;
- confidentiality restrictions;
- publication permissions;
- redaction instructions.

13.2 Third-party data

The Enterprise shall not include third-party data unless it has the right to:

- provide it to EMJ.LIFE;
- authorise Processing;
- include it in a Compendium;
- provide it to intended recipients;
- permit the selected DOI status;
- retain and use the delivered archive.

13.3 Conflicting rights

If a third party restricts publication or disclosure, the Enterprise shall notify EMJ.LIFE before production. EMJ.LIFE may:

- exclude the material;
- redact the material;
- restrict access;
- change the DOI status;
- request additional permission;
- delay production;
- reject the affected scope.

14. Privacy and Personal Data

Personal Data in a Compendium shall be governed by the DPA and Security Schedule. The Enterprise shall identify:

- unnecessary Personal Data;
- sensitive Personal Data;
- data requiring redaction;
- data requiring restricted access;
- data subject to third-party restrictions;
- data that must not be published.

EMJ.LIFE may require:

- redaction;
- masking;
- minimisation;
- access restriction;
- separate approval;
- exclusion;
- anonymisation.

A request to publish a Compendium shall not override:

- Data Subject rights;
- confidentiality;
- legal restrictions;
- third-party rights;
- regulatory requirements;
- security controls.

15. Review, Scope and Acceptance

15.1 Pre-production review

EMJ.LIFE shall review:

- evidence-period eligibility;
- continuity;
- identity;
- scope;
- data completeness;
- permissions;
- duplicate records;
- integrity;
- publication status;
- delivery requirements.

15.2 Scope changes

The Enterprise may request a scope change before production is finalised. A scope change may affect:

- fee;
- delivery date;
- evidence period;
- DOI status;
- data review;
- redaction;
- version number;
- eligibility.

EMJ.LIFE may require a new application or additional fee.

15.3 Enterprise review period

The Enterprise has ten Business Days after complete accessible delivery to notify a material missing core item, corrupt file, scope/version/integrity mismatch or unauthorised access/publication. A purported delivery with inaccessible required files or an unregistered required DOI does not start deemed acceptance of the missing scope unless an alternative is expressly accepted.

Identify the affected record/version and supporting detail. The notice does not authorise the Enterprise to alter the issued original or retrospectively impose unagreed scope.

15.4 Limited deemed acceptance

If no material delivery issue is notified within the ten-Business-Day review period after complete delivery, delivery is deemed accepted. This does not waive proven latent production errors, confidentiality/privacy rights, fraud, mandatory rights, correction obligations or accrued remedies, and does not convert the Compendium into an external assurance or compliance conclusion.

16. Corrections and Supersession

16.1 Correction request

The Enterprise may request correction of:

- factual errors;
- version errors;
- incorrect relationships;
- incorrect dates;
- missing agreed items;
- incorrect access status;

- material file-integrity issues.

The request shall include:

- Compendium identifier;
- version;
- affected file or record;
- explanation;
- supporting information;
- requested correction.

16.2 Correction procedure and timing

Acknowledge a complete correction request within two Business Days and determine a demonstrable material production error within five Business Days. Correct an accepted provider production error within seven calendar days after verification, or agree a reasoned schedule where a required external registrar correction prevents that period; the long-stop/refund remedy in Section 7.2 applies to material undelivered/corrupt required scope.

Issue an attributable corrected/superseding version, preserve lawful prior metadata/history, update manifest/DOI status and delivery records, and notify affected authorised recipients where necessary. Do not retain unlawful personal payload solely to preserve a prior version. Customer-requested new scope uses a separately accepted fee/date, not an undisclosed correction charge.

16.3 No silent overwrite

A corrected Compendium shall not silently overwrite a prior version where the prior version is relevant to:

- Historical Records;
- auditability;
- dispute handling;
- legal retention;
- delivery history;
- evidence continuity.

16.4 Correction fee

A correction caused solely by EMJ.LIFE's demonstrable production error shall not incur an additional production fee. A correction caused by:

- new Enterprise information;
- changed Enterprise instructions;
- changed scope;
- late permission;
- changed publication status;
- inaccurate original submission;
- Enterprise-requested redesign;

may incur an additional fee and revised delivery date.

17. Version, status and publication governance

Each Compendium has a persistent ID, version, issue date, approved evidence period, rights/access boundary, manifest, integrity and delivery record. A later issuance does not automatically invalidate an earlier valid period.

Use publication/evidence states ACTIVE, SUPERSEDED, HISTORICAL and WITHDRAWN. Pending DOI registration is PENDING_REGISTRATION and is not a delivered registered record. Corrected and Disputed are attributable correction/review annotations; archival is a storage treatment; Restricted is account/payload access. Maintain the SEC Section 16 domain distinctions rather than treating those labels as interchangeable.

Every change records the prior state, actor/authority, reason, source record and effective time. Preserve lawful minimal history and version relationships, subject to DPA deletion and rights. Never silently overwrite a relevant issued record.

18. Cancellation, Delay and Rejection

18.1 Enterprise cancellation

Before production starts, the Enterprise may cancel and receive its paid Compendium fee within thirty calendar days. No unpriced administrative deduction applies. After production starts, convenience cancellation is ordinarily non-refundable; separately agreed completed bespoke work is governed by its own accepted scope.

Provider error, missed required delivery, confidentiality/privacy breach, legally required refund and the Section 7.2 long-stop remedy are not convenience cancellation. Acceptance does not remove correction rights for a proven production error.

18.2 Reasoned rejection or lawful protective hold

Reject an ineligible, unlawful, unpermissioned, materially inaccurate or technically unproducible request with the specific scope/reason and any available corrective path, ordinarily at pre-production review. A temporary protective hold follows Section 7.2's recorded notice and review; it is not indefinite forfeiture of payment.

No request is accepted as a registered DOI service without the required metadata/publication rights. If EMJ.LIFE later cannot perform an accepted lawful request for provider-side reasons, apply Section 18.3 and the delivery long-stop remedy. Costs from proven Enterprise breach remain subject to actual contractual/legal remedies, not an unrecorded blanket fee confiscation.

18.3 Refund and accepted alternative

If EMJ.LIFE rejects an unproduced request, cannot provide accepted core scope for provider-side reasons, or the Enterprise exercises the Section 7.2 non-delivery remedy, refund the related standard Compendium fee within thirty calendar days. Any alternative credit, corrected application or partial delivery with fee adjustment requires the Enterprise's express acceptance.

For Enterprise-caused unlawful/misleading material discovered after production begins, retain only the fee lawfully due for conforming work already performed under the accepted scope; explain any proposed deduction and its basis. Mandatory rights, proven claims and production-error correction remain unaffected. A written amendment may settle a disputed deduction; unilateral discretion does not replace it.

19. Relationship with Points and Score

A Compendium may describe attributable EGC ID, task, Node, Point and Score history within the approved scope. Production/payment/publication neither consumes nor awards E-IPP and does not prove an external rating. Only approved separately activated supply-chain task outcomes earn the fixed award in EIPP Section 6.3.

A DOI does not revive expired Points, change the annual cycle, bypass task reissuance rules or manufacture continuity. No Compendium-related Point charge or bonus is included in this v1.0 package.

20. Subscription end and accepted production

An already accepted, paid and eligible request for an approved historical period continues under its production/delivery obligations even if the Subscription later ends; completion is not new governed task activity or retroactive extension of that period. A legal/rights restriction follows the recorded pause/refund process.

New requests after actual cessation require express acceptance of a lawful historical scope; no new active evidence period is implied. Delivered-file use survives under DRE Section 4.2. Download access, personal-data deletion and minimum DOI publication identity are separately governed by Sections 10/11 and the DRE/DPA.

21. External Use and Disclaimers

The Enterprise may use a delivered Compendium only in a manner that is:

- accurate;
- complete in context;
- consistent with access status;
- consistent with third-party permissions;
- consistent with limitation statements;
- compliant with law;
- consistent with the Agreement.

The Enterprise shall not represent that:

- EMJ.LIFE audited the Enterprise;
- EMJ.LIFE assured the Enterprise;
- EMJ.LIFE certified the Enterprise;
- the Compendium proves legal compliance;
- the Compendium proves sustainability performance;
- the Compendium proves carbon achievement;
- the Compendium proves supplier quality;
- the DOI proves external verification;
- the JSON file is a regulatory filing;
- the Compendium is an official report of IFRS Foundation, ISSB or SASB;
- the Compendium is endorsed by a government or regulator.

22. Security and Confidentiality

The Compendium shall be subject to:

- the DPA;
- the Security Schedule;
- confidentiality obligations;
- access controls;
- encryption requirements;
- publication restrictions;
- retention and exit controls.

The Enterprise shall protect:

- JSON evidence files;
- DOI credentials;

- encrypted archives;
- encryption keys;
- manifests;
- delivery records;
- internal copies;
- third-party confidential information.

23. Service Commitment Boundary

EMJ.LIFE is accountable for reasoned eligibility/scope review, the defined seven-calendar-day delivery obligation and long-stop remedies, all core items, secure access and delivery, registration/publication instructions, attributable versions and prompt correction of provider production errors.

External search indexing, regulator/auditor/investor/customer acceptance, underlying Enterprise data truth and ungranted third-party rights are not guaranteed. Those external boundaries do not excuse the provider's own delivery, permissions verification, data-protection, security, refund or correction duties.

24. Term and Survival

This Schedule begins when the applicable Enterprise Contract and Governance Pack becomes effective and applies to each accepted Compendium request. The following obligations survive termination or delivery:

- confidentiality;
- data protection;
- security;
- ownership;
- use restrictions;
- DOI access status;
- version and integrity records;
- correction and supersession;
- Historical Records;
- legal retention;
- disclaimers;
- service commitment boundaries;
- payment obligations;
- dispute rights.

25. 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 the Compendium Schedule and agree that it governs a separately accepted optional request. This acknowledgement does not order the service, authorise a charge or approve public release of evidence.

Default purchase status: not purchased. A separate eligible request, express purchase acceptance and applicable publication instructions are required under this Schedule.

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.

The CPS acknowledgement counts as one of the seven Stage Two document acknowledgements. It accepts the conditional terms for a later separately accepted request; it does not purchase a Compendium or authorise payment or public payload release.