Vendor Security Questionnaire

Movahedi Solutions, 1000823315 ONTARIO INC., Mississauga, Ontario, Canada

Date: October 27-28, 2026 | Contact: mohammad@movahedi.ca

Document details

- Vendor: 1000823315 ONTARIO INC., operating as Movahedi Solutions
- Site in scope: movahedi.ca
- Date of this document: Oct 27-28, 2026
- Contact for a tailored response: mohammad@movahedi.ca
- How to use this document: Find the category in the table of contents, read the plain answer first, then read the evidence and detail that follow it. A buyer who stops after the first paragraph of an answer still has the answer. A buyer who keeps reading has the proof, the limits, and the related sections to check next.
- Scope note: This questionnaire covers two things, and it keeps them separate. The first is the public site movahedi.ca, a live public site that stores no client data on it. The second is advisory engagement work, where client material is handled only for that engagement under the rules in Category B and Category L. Where a question fits only one of those two, the answer says so.
- Where the evidence is short, the section is short, and the answer says why. Short sections in this document mean the evidence is short, not that the check was skipped. No answer in this document invents a certification, a client, a testimonial, a metric, a logo, an uptime figure, a service level figure, an encryption standard, a residency location, a retention period, a backup schedule, or a monitoring tool.

Summary counts

Total questions: 60

- Answered with evidence: 23
- Answered not held: 18
- Answered not applicable: 4
- Answered to be confirmed in writing per engagement: 15

Total: 23 + 18 + 4 + 15 = 60

Status meanings used in every answer:

- Answered with evidence: the answer is supported by a dated source named in that answer.
- Answered not held: the vendor does not hold the item asked about, and the answer says so

plainly.

- Answered not applicable: the question does not fit this service model, and the answer gives the reason.
- Answered to be confirmed in writing per engagement: the answer depends on the terms of a specific engagement, and it must be confirmed in writing for that engagement. It is not stated here as a general claim.

Table of contents

1. How this document was prepared
2. Evidence index: dated entries
3. Category A: Company and services (A1 to A5)
4. Category B: Client data handling (B1 to B5)
5. Category C: Access control (C1 to C5)
6. Category D: Infrastructure and hosting (D1 to D5)
7. Category E: Website security (E1 to E5)
8. Category F: Vulnerability management, change, and backups (F1 to F5)
9. Category G: Incident response (G1 to G5)
10. Category H: Compliance, certifications, insurance, and clearance (H1 to H5)
11. Category I: Privacy and regulation (I1 to I5)
12. Category J: Subprocessors and third parties (J1 to J5)
13. Category K: Business continuity and availability (K1 to K5)
14. Category L: People, physical security, and contract terms (L1 to L5)
15. Cross-link index
16. Request route for a tailored response
17. Improvement note: review, refresh, and addition over the next year

1. How this document was prepared

This document is part of the Trust Center for Movahedi Solutions. No earlier Trust Center version date is claimed in this document, and no longer history is claimed for the Trust Center itself.

The work behind the Trust Center accumulated in a different way from the Trust Center versions. The site movahedi.ca was built and improved over many sessions before Oct 27-28, 2026. The exact date of each earlier site session is not stated in this document, because a date that is not known is not given here. The pattern of that work is stated, and the outcomes that can be checked today are stated with their dates: a live public site, delivery over HTTPS, and a third-party header

scan on Oct 28, 2026.

Registrations and third-party profiles in this document are dated Oct 27, 2026. Each one is listed as its own dated entry in Section 2, not as a shared row, so a buyer can check each entry on its own.

The Privacy Policy for the public site is dated separately. Its last update date is July 15, 2026. That date is older than the Trust Center v4 date, and it is shown as it stands, not moved forward to match this document.

The header scan is dated Oct 28, 2026, 00:59 UTC. It is the most recent dated technical evidence in this document. It is labelled in every place it appears as a header scan, never as a penetration test, because a header scan and a penetration test are different checks.

2. Evidence index: dated entries

Each entry below is a separate dated record. A question that relies on an entry names that entry again in its evidence paragraph.

2.1 Public site

- Entry: movahedi.ca, live public site.
- Date in this document: Oct 27-28, 2026.
- Source: live public site at https://movahedi.ca
- Detail: The site is built and deployed from GitHub and delivered through Cloudflare over HTTPS. No specific GitHub plan and no specific Cloudflare plan is claimed in this document.

2.2 Third-party header scan

- Entry: Security Headers scan of movahedi.ca.
- Date: Oct 28, 2026, 00:59 UTC.
- Source: third-party scan at https://securityheaders.com/?q=https://movahedi.ca&followRedirects=on
- Result: grade A+.
- Headers passed: Strict-Transport-Security with preload, Content-Security-Policy, Permissions-Policy, Referrer-Policy, X-Content-Type-Options, X-Frame-Options.
- Limit: This is a header scan only. It is not a penetration test, and it is not presented as one anywhere in this document.

2.3 Privacy Policy

- Entry: Privacy Policy for movahedi.ca.
- Date: last updated July 15, 2026.
- Source: Privacy Policy for the public site, as published on movahedi.ca.
- Detail: The policy date is stated here as July 15, 2026. No later policy date is claimed.

2.4 Registration: UNGM

- Entry: UNGM Basic registration.
- Identifier: 1295964.
- Date in this document: Oct 27, 2026.
- Detail: Listed as a registration only. It is not a certification, and it is not presented as one.

2.5 Registration: MERX

- Entry: MERX Basic Free registration.
- Date in this document: Oct 27, 2026.
- Detail: Listed as Basic Free, with no paid subscription claim and no payment method claim.

2.6 Registration: CanadaBuys and SAP Ariba

- Entry: CanadaBuys supplier profile route through SAP Ariba.
- Identifier: AN11542201146.
- Date in this document: Oct 27, 2026.
- Detail: Listed as a registration identifier only. It is not a certification, and no clearance claim follows from it.

2.7 Registration: CPSS ePortal

- Entry: CPSS ePortal registration.
- Date in this document: Oct 27, 2026.
- Detail: Listed as a registration only. No outcome beyond registration is claimed from this entry alone.

2.8 Registration: Ontario Tenders Portal

- Entry: Ontario Tenders Portal registration.
- Date in this document: Oct 27, 2026.

- Detail: Listed as a registration only. No contract, award, or outcome is claimed from this entry.

2.9 Third-party profile: LinkedIn Services

- Entry: LinkedIn Services profile for Movahedi Solutions.
- Date in this document: Oct 27, 2026.
- Detail: Listed as a third-party profile only. No client, testimonial, or outcome is claimed from this entry.

2.10 Third-party profile: Catalant

- Entry: Catalant profile for Movahedi Solutions.
- Date in this document: Oct 27, 2026.
- Detail: Listed as a third-party profile only. No client, testimonial, or outcome is claimed from this entry.

2.11 Third-party profile: Clutch

- Entry: Clutch profile for Movahedi Solutions.
- Date in this document: Oct 27, 2026.
- Review count: 0 reviews.
- Detail: The count is stated as 0. No review, rating claim beyond the count, testimonial, or client name is added to it.

2.12 Third-party profile: Trustpilot

- Entry: Trustpilot profile for Movahedi Solutions.
- Date in this document: Oct 27, 2026.
- Review count: 0 reviews.
- Rating shown in the record: 0.0.
- Detail: The count and the rating are stated as they stand. No review text, testimonial, or client name is added to them.

2.13 Personal credentials, personal only

- Entry: Personal credentials.
- Credentials: ISC2 CC, CIPP/C, Six Sigma Black Belt.
- Date in this document: date of each credential is not stated in this document.
- Detail: These are personal credentials of the founder. They are not company certifications, and

no company certification is claimed from them.

2.14 Trust Center versions

- Entry: Trust Center v1, v2, v3, and v4.
- Date: Oct 27, 2026.
- Detail: The progression falls on Oct 27, 2026. This questionnaire is prepared for Trust Center v4, for linking from the Trust Center Documents section and the Security Questionnaire Answers section.

How each answer is written

Every answer below follows the same order, so a buyer can stop early or read on with the same expectation each time:

- Answer first, in plain language.
- Evidence next, with a date and a source, and a link where one exists.
- Detail next, covering scope, limits, and what is not claimed.
- Related links last, naming the Trust Center section, policy, document, registration, third-party profile, or other questionnaire answer that carries the same thread. A related name is a pointer to check, not a second claim.

Legal reading note, applied to every answer: This document is company information for procurement and security review. It is not legal advice for a specific client matter, and it is not a law firm opinion. Where a matter depends on a specific engagement, the answer says it must be confirmed in writing per engagement, before work starts where that timing matters. That confirmation step is part of the answer, not an omission from it.

Category A: Company and services

A1. What is the legal name, trade name, location, and business type of the vendor? [Answered with evidence]

Answer: The vendor is 1000823315 ONTARIO INC., operating as Movahedi Solutions, an independent privacy and AI governance consultancy based in Mississauga, Ontario, Canada.

Evidence: Company record in this document, dated Oct 27, 2026. Site in scope: https://movahedi.ca

Detail: The legal name and the trade name are both given, so a buyer can match procurement records to the correct entity. The business type is stated as an independent consultancy, which sets the scope for the rest of this questionnaire: this is an advisory firm, not a hosted software provider, not a data centre operator, and not a reseller. No parent company, subsidiary, or group structure is claimed in this document. Staffing for a specific engagement is covered separately in A4, where its status is stated plainly.

Related: Trust Center Documents section; Trust Center Security Questionnaire Answers section; A4; A5; L5.

A2. What services does the vendor provide? [Answered with evidence]

Answer: Privacy and AI governance work, Law 25 compliance support, EU AI Act readiness assessments, privacy advisory, knowledge-base work, AI and agent inventories, custom AI governance frameworks, and risk assessments.

Evidence: Service record in this document, dated Oct 27, 2026. Site in scope: https://movahedi.ca

Detail: Each service is an advisory service, delivered as analysis, frameworks, inventories, and assessments. Law 25 compliance support and EU AI Act readiness assessments are services, not certifications and not client outcomes. No result for a specific client is claimed from listing a service, and no client name is attached to any service in this document. The work pattern behind these services is legal research and governance analysis: reading the relevant law and guidance, mapping it to a client's activities and data, and producing a framework, inventory, or assessment the client can act on. That pattern is stated here in general terms only, with no meeting, room, or client specifics.

Related: Trust Center Documents section; I1; I2; I3; J2; L5.

A3. What is the contact route for security, privacy, and procurement questions? [Answered with evidence]

Answer: mohammad@movahedi.ca.

Evidence: Contact record in this document, dated Oct 27, 2026. Site in scope: https://movahedi.ca

Detail: One contact route is given for all three kinds of question, so a buyer does not need to guess which address fits a security question versus a procurement question. This route is also the route for a tailored response, for incident notice under G2, and for the per-engagement confirmations described in this document. No phone number, portal, or ticket system is claimed as a security contact route in this document, because none is stated in the evidence stated in this document.

Related: Trust Center Documents section; G2; L5; Section 16, Request route for a tailored response.

A4. How large is the vendor, and how is it staffed? [Answered to be confirmed in writing per engagement]

Answer: Movahedi Solutions is an independent consultancy. Staffing for a specific engagement, including who will work on it and what they will cover, is agreed in writing for that engagement.

Evidence: Business type record in this document, dated Oct 27, 2026.

Detail: Evidence for this answer is limited to the items stated below. The independent consultancy shape is stated, and the rest is left for per-engagement confirmation. For a buyer, the practical effect is clear: staffing for an engagement, including who will work on it and what screening or security steps apply to those people, must be confirmed in writing before work starts. That confirmation is where L1 and L2 connect to this answer.

Related: Trust Center Documents section; H4; L1; L2.

A5. What registrations and third-party profiles does the vendor hold? [Answered with evidence]

Answer: The vendor holds the registrations and third-party profiles listed as separate dated entries below. Each entry is a registration or a profile only, not a certification and not a contract award.

Evidence: Dated entries in Section 2.4 to Section 2.12, all dated Oct 27, 2026, plus the site at https://movahedi.ca

Detail: The entries are given one by one, so each can be checked on its own:

- UNGM Basic, identifier 1295964, dated Oct 27, 2026. Registration only.
- MERX Basic Free, dated Oct 27, 2026. Basic Free only, with no paid subscription claim and no payment method claim.
- CanadaBuys route through SAP Ariba, identifier AN11542201146, dated Oct 27, 2026. Registration identifier only.
- CPSS ePortal registration, dated Oct 27, 2026. Registration only.
- Ontario Tenders Portal registration, dated Oct 27, 2026. Registration only.
- LinkedIn Services profile, dated Oct 27, 2026. Profile only.
- Catalant profile, dated Oct 27, 2026. Profile only.
- Clutch profile, dated Oct 27, 2026, with 0 reviews. Count stated as 0, with no review text added.

• Trustpilot profile, dated Oct 27, 2026, with 0 reviews and a rating of 0.0 in the record. Count and rating stated as they stand, with no review text added.

No entry in this list is used to imply a client relationship, an award, a testimonial, or a clearance. A buyer who needs the current status of any single entry should ask for a fresh confirmation for that entry, using the route in Section 16.

Related: Trust Center Documents section; Trust Center Registrations section; H1; H2; H3; J1.

Category B: Client data handling

Legal scope note for this category: The rules below are company rules for handling client material. They set the default position for an engagement. Where a client needs a different rule, a stricter rule, or a specific security, screening, or insurance requirement, that rule must be confirmed in writing per engagement, before work starts. This category does not give legal advice for a specific client matter.

B1. What client data does the public site movahedi.ca store? [Answered with evidence]

Answer: None. The public site stores no client data on it.

Evidence: Site scope record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: This answer covers the public site only, and it is the reason several later answers are marked not applicable. A public advisory site is not a client data store, not a client portal, and not a hosted application holding client records. Engagement material is handled separately from the public site, under B2 and B5. A buyer assessing the public site therefore assesses a site with no client data on it, while a buyer assessing an engagement assesses the engagement rules in this category.

Related: Trust Center Security Practices section; Trust Center Privacy Policy section; C5; D5; F3.

B2. How may client engagement material be used? [Answered with evidence]

Answer: Client material is used only for its own engagement. It is not sold, it is not used for model training, and it is not used for any unrelated purpose.

Evidence: Client data rules record in this document, dated Oct 27, 2026.

Detail: The limit is stated as a use limit, not only as a storage limit. Use only for its engagement

means the material does not move to another engagement, to marketing, to a public example, or to training data. No sale means no transfer of client material for payment or other value to an unrelated party. No model training use means client material is not fed into model training, whether for the vendor's own models or for a third party's models. If an engagement needs a use beyond this default, that use must be confirmed in writing per engagement, before the material is used that way. Silence is not consent to a wider use.

Related: Trust Center Documents section; Trust Center Privacy Policy section; B5; I5; J5.

B3. What retention period applies to client engagement material? [Answered to be confirmed in writing per engagement]

Answer: No fixed retention period is stated in this document. The retention period for an engagement must be confirmed in writing per engagement.

Evidence: No retention period record is stated in the evidence stated in this document, dated Oct 27, 2026. The end-of-engagement rule in B5 is the only retention-related rule stated generally.

Detail: This answer is deliberately not filled with a number of days, months, or years, because no such period is verified in the evidence stated in this document. Inventing a period would be worse than leaving it for confirmation, since a buyer would then rely on a figure with no source. The default end position is in B5: material is removed at the end of the engagement, and returned or deleted on client instruction. A client who needs a specific retention period, a hold period, or a deletion deadline should set it in writing for that engagement, before work starts, and that written period then governs that engagement.

Related: Trust Center Documents section; B5; F5; L5.

B4. Where is client engagement material stored, and what residency applies? [Answered to be confirmed in writing per engagement]

Answer: No residency location is stated in this document. Storage location and residency for an engagement must be confirmed in writing per engagement.

Evidence: No residency location record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Residency is a legal and contractual question as much as a technical one, since it can affect which privacy law applies and which transfer rules apply. For that reason, this document does not name a country, region, or data centre for client engagement material. A buyer who needs a

residency commitment, a transfer restriction, or a named storage location should require it in writing for that engagement, before material is shared. The public site position is separate and is covered in D1 and D4: the public site is delivered through Cloudflare over HTTPS, with no client data on it under B1, so no client residency claim is made for the public site either.

Related: Trust Center Documents section; D1; D4; J2; L5.

B5. What happens to client material at the end of an engagement, or on client instruction? [Answered with evidence]

Answer: Client material is removed at the end of the engagement, and it is returned or deleted on client instruction.

Evidence: Client data rules record in this document, dated Oct 27, 2026.

Detail: Two triggers are given, and both are client-controlled in effect. End of engagement triggers removal as the default. Client instruction triggers return or deletion, as the client directs. Return and deletion are stated as alternatives chosen by the client, not as a vendor choice made for the client. The timing and the proof of return or deletion for a specific engagement, for example a confirmation note or a deletion record, must be confirmed in writing per engagement, because this general rule does not by itself state a deadline or a proof format. No copy is retained for an unrelated purpose after removal under B2.

Related: Trust Center Documents section; B2; B3; J5; L5.

Category C: Access control

C1. Who can access client engagement material? [Answered with evidence]

Answer: Access is limited to the people working on that engagement.

Evidence: Client data rules record in this document, dated Oct 27, 2026.

Detail: Limited access is the general rule, and it is tied to the engagement, not to the firm as a whole. Material for one engagement is not open to people working only on another engagement, and it is not open for general browsing. The named people, their roles, and any client approval step for adding a person must be confirmed in writing per engagement, because this general rule does not name individuals. That per-engagement confirmation is also where screening requirements under L1 connect to access: a client who needs a screening step should set it before access is granted, not after.

Related: Trust Center Security Practices section; A4; L1; J2.

C2. Is multi-factor authentication used for accounts that can reach engagement material or site accounts? [Answered to be confirmed in writing per engagement]

Answer: No multi-factor authentication claim is made in this document. The authentication controls for a specific engagement, including whether multi-factor authentication applies and to which accounts, must be confirmed in writing per engagement.

Evidence: No authentication control record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Evidence for this answer is limited to the items stated below. Site account controls for GitHub and Cloudflare were not verified from live configuration in this document, so no setting is claimed for them here. A buyer who needs a multi-factor authentication commitment should require it in writing for that engagement, naming the accounts and the method, before material is shared. A general statement that multi-factor authentication is used somewhere would not answer that question, so none is given.

Related: Trust Center Security Practices section; C3; C4; D1.

C3. What password and single sign-on rules apply? [Answered to be confirmed in writing per engagement]

Answer: No password rule and no single sign-on rule is stated in this document. Both must be confirmed in writing per engagement where they apply to that engagement.

Evidence: No password or single sign-on record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: The public site has no visitor login, so no visitor password rule arises from the public site itself, as stated in C5. Engagement accounts, shared folders, and tools used for a specific engagement are a separate matter, and their password and sign-on rules depend on the tools agreed for that engagement. Those rules must be set in writing for that engagement, before access is granted. No password length, rotation, or sign-on provider is named here, because none is verified in the evidence stated in this document.

Related: Trust Center Security Practices section; C2; C5; J2.

C4. How often is access reviewed, and how is access removed when a person leaves an engagement? [Answered to be confirmed in writing per engagement]

Answer: No review frequency and no removal timetable is stated in this document. Both must be confirmed in writing per engagement.

Evidence: No access review record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Access review and removal matter most at the points where risk changes: a person joins, moves, or leaves an engagement, and an engagement ends. The general rule in C1 limits access to people working on the engagement, and B5 removes material at engagement end, but neither states a review date or a removal deadline. A buyer who needs a review cadence, a removal deadline, or a confirmation of removal should set it in writing for that engagement, before work starts. This keeps the commitment tied to the engagement where it can be checked, rather than stated as a general figure with no source.

Related: Trust Center Security Practices section; B5; C1; L1.

C5. How are visitor or client accounts provisioned on movahedi.ca? [Answered not applicable]

Answer: They are not provisioned, because the public site has no visitor or client accounts.

Evidence: Site scope record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: A question about account provisioning assumes accounts exist. On a public site with no login for visitors and no client portal, that assumption does not hold. There is no joiner, mover, or leaver process for public site visitors, because there is no visitor account to join, move, or leave. Engagement access is a separate matter and is covered in C1 to C4, where per-engagement confirmation applies. Marking this answer not applicable is more accurate than inventing an account process for a site that has no accounts.

Related: Trust Center Security Practices section; B1; C1; C3.

Category D: Infrastructure and hosting

D1. How is movahedi.ca built, deployed, and delivered? [Answered with evidence]

Answer: The site is built and deployed from GitHub, and it is delivered through Cloudflare over

HTTPS.

Evidence: Technology record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: The pattern is source control plus managed delivery. Source and deployment sit with GitHub, so the site can be rebuilt from source. Delivery sits with Cloudflare, over HTTPS, so visitors reach the site over an encrypted transport. The site was built and improved over many sessions before Oct 27-28, 2026, with the exact date of each earlier session not stated in this document. No self-managed server is claimed in this model, which is why F3 is marked not applicable. No specific GitHub plan and no specific Cloudflare plan is claimed, as stated in D2.

Related: Trust Center Security Practices section; D2; E1; F1; K5.

D2. What GitHub and Cloudflare plans are used? [Answered not held]

Answer: No specific plan is claimed in this document for GitHub or for Cloudflare.

Evidence: No plan record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Evidence for this answer is limited to the items stated below. The providers are named in D1, because the delivery model depends on them, but the commercial plan tier for each provider is not stated in the evidence stated in this document, so it is not stated here. A buyer who needs a plan tier, a feature tied to a tier, or a provider term should ask for a fresh confirmation for that provider, using the route in Section 16. A plan tier stated without a source would not help a buyer check it, so none is given.

Related: Trust Center Security Practices section; D1; J1.

D3. What encryption standard applies to client engagement material? [Answered to be confirmed in writing per engagement]

Answer: No encryption standard for client engagement material is claimed in this document. The encryption and transfer method for an engagement must be confirmed in writing per engagement.

Evidence: No encryption standard record for client material is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: This answer must be kept separate from the public site position. For the public site, delivery over HTTPS is stated in D1 and E1, and the header scan in E2 confirms Strict-Transport-Security with preload. That site transport position does not by itself state an encryption standard for client engagement material sent or stored during an engagement. The engagement method, including how files are transferred and how stored material is protected, must be agreed in writing for that

engagement, before material is shared. No standard name, key length, or algorithm is given here, because none is verified for client material in this document.

Related: Trust Center Security Practices section; D1; E1; E2; J2.

D4. Where is the site hosted, and where is client material held? [Answered to be confirmed in writing per engagement]

Answer: No hosting location and no client material location is stated in this document. Both must be confirmed in writing per engagement where a location commitment is needed.

Evidence: No location record is stated in the evidence stated in this document, dated Oct 27, 2026. Site: https://movahedi.ca

Detail: The delivery providers are named in D1, but a provider name is not a location. Cloudflare delivery and GitHub source control do not by themselves state a single hosting location for the public site, and they do not state a location for engagement material. For the same legal reason given in B4, a location commitment for engagement material belongs in the written terms for that engagement, before material is shared. No data centre name, city, or country is added here for either the site or engagement material.

Related: Trust Center Security Practices section; B4; D1; J1.

D5. How is client data separated from other clients in a shared system? [Answered not applicable]

Answer: There is no shared client system to separate, because the public site stores no client data and no multi-tenant hosted application is claimed.

Evidence: Site scope record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: Separation controls assume a shared store where one client's data sits beside another client's data. That model does not fit an advisory firm whose public site holds no client data under B1, and whose engagement material is limited to its own engagement under B2. Separation in this model is engagement separation: material is used only for its engagement, access is limited to people working on that engagement under C1, and material is removed at engagement end under B5. A buyer who needs a technical separation statement for a hosted system should not rely on this answer, because no such hosted system is claimed.

Related: Trust Center Security Practices section; B1; B2; C1.

Category E: Website security

E1. Is movahedi.ca served over HTTPS? [Answered with evidence]

Answer: Yes. The site is served over HTTPS.

Evidence: Technology record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: HTTPS delivery is the transport position for the public site, and it is consistent with the header scan result in E2, which passed Strict-Transport-Security with preload. HTTPS for the public site does not by itself answer the engagement encryption question in D3, and it is not used here as if it did. The two questions are kept separate: site transport is evidenced here, engagement material protection is confirmed per engagement under D3.

Related: Trust Center Security Practices section; D1; E2; D3.

E2. What independent check supports the site security header position? [Answered with evidence]

Answer: A third-party header scan by Security Headers, grade A+, dated Oct 28, 2026, 00:59 UTC.

Evidence: Third-party header scan, dated Oct 28, 2026, 00:59 UTC, at https://securityheaders.com/?q=https://movahedi.ca&followRedirects=on

Detail: This is a header scan only. The grade and the date are stated, and the scan link is given so a buyer can re-run or re-check the same scan. The scan is the most recent dated technical evidence in this document, and it postdates the Trust Center v4 date of Oct 27, 2026 by one day, which is why the document date is given as Oct 27-28, 2026. No wider security claim is drawn from this scan than the headers it checked, and the header list is given in full in E3.

Related: Trust Center Security Practices section; Trust Center Documents section; E1; E3; E4.

E3. Which security headers passed in that scan? [Answered with evidence]

Answer: Strict-Transport-Security with preload, Content-Security-Policy, Permissions-Policy, Referrer-Policy, X-Content-Type-Options, and X-Frame-Options all passed.

Evidence: Third-party header scan, dated Oct 28, 2026, 00:59 UTC, at https://securityheaders.com/?q=https://movahedi.ca&followRedirects=on

Detail: Each header is named, rather than summarised as headers in general, so a buyer can match the list to the scan result. Strict-Transport-Security with preload means the site asks

browsers to use HTTPS, including on first visit where preload applies. Content-Security-Policy, Permissions-Policy, Referrer-Policy, X-Content-Type-Options, and X-Frame-Options each constrain a different browser behaviour, and all six are recorded as passed in the same scan. No header value, policy text, or configuration detail beyond the passed list is stated here, because no such detail is given in the scan summary record in this document. A buyer who needs the full header values should re-run the scan at the link above and compare the live result to this dated result.

Related: Trust Center Security Practices section; E1; E2; E4.

E4. Has movahedi.ca had a penetration test? [Answered not held]

Answer: No penetration test is claimed in this document.

Evidence: No penetration test record is stated in the evidence stated in this document, dated Oct 27-28, 2026. The only dated technical check in this document is the header scan in E2.

Detail: The distinction matters, and it is kept explicit in every place the scan appears. A header scan checks response headers. A penetration test probes for exploitable weaknesses. One is not the other, and a grade A+ on a header scan does not become a penetration test result by being repeated. A buyer who needs a penetration test should require it as a separate, written commitment, with scope, tester, date, and findings handling agreed before work starts. Until such a test exists and is recorded, this answer stays not held.

Related: Trust Center Security Practices section; E2; E3; F4.

E5. What monitoring tool watches the public site? [Answered not held]

Answer: No monitoring tool is named in this document.

Evidence: No monitoring tool record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Evidence for this answer is limited to the items stated below. Naming a tool without a verified configuration record would give a buyer a name to trust with no way to check it. The dated evidence that does exist for the public site is the live site itself and the Oct 28, 2026 header scan in E2. Monitoring, alerting, and log review for a specific engagement, where they apply, must be confirmed in writing per engagement, as covered in F4 and F5. No uptime figure follows from this answer, and none is claimed in K1 either.

Related: Trust Center Security Practices section; E2; F4; K1.

Category F: Vulnerability management, change, and backups

F1. How is site source controlled and deployed? [Answered with evidence]

Answer: Site source and deployment sit with GitHub, and delivery sits with Cloudflare over HTTPS.

Evidence: Technology record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: The pattern is a managed source and delivery chain, not a hand-edited live server. Changes go through source control, deployment comes from that source, and delivery comes through Cloudflare. That pattern also supports recovery of the public site: the site can be rebuilt from source, rather than depending on a single live copy. The exact review step for each change is covered separately in F2, where its status is stated plainly, so this answer does not overstate F1 into a full change approval claim.

Related: Trust Center Security Practices section; D1; F2; K2.

F2. What change approval process applies to site and engagement changes? [Answered to be confirmed in writing per engagement]

Answer: No change approval process is stated generally in this document. The process for a specific engagement must be confirmed in writing per engagement.

Evidence: No change approval record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Site changes and engagement changes are different, and the answer keeps them separate. For the site, the source control pattern in F1 is stated, but a named approver, a review checklist, or a release gate is not stated, because none is verified in the evidence stated in this document. For an engagement, the change process, including who approves a framework change, an inventory change, or a scope change, depends on the engagement and must be agreed in writing before work starts. A buyer who needs a change log or an approval record for an engagement should require that record format in the written terms.

Related: Trust Center Documents section; F1; A2; L5.

F3. What patching schedule applies to vendor-managed servers? [Answered not applicable]

Answer: No patching schedule applies, because no self-managed server is claimed in this model.

Evidence: Technology record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: Patching assumes a server the vendor manages and patches. The model in D1 uses GitHub for source and deployment and Cloudflare for delivery, with no self-managed server in scope. Platform patching for those providers sits with those providers, and no provider patching schedule is claimed here. Engagement work does not add a vendor-managed server either, since no hosted application is claimed in D5. A buyer assessing patching should therefore assess the provider model in D1, not a vendor server schedule that does not exist in this model.

Related: Trust Center Security Practices section; D1; D5; J1.

F4. What vulnerability scanning schedule and tool are used? [Answered not held]

Answer: No vulnerability scanning schedule and no scanning tool are claimed in this document.

Evidence: No scanning schedule or tool record is stated in the evidence stated in this document, dated Oct 27, 2026. The dated technical check that does exist is the header scan in E2.

Detail: The header scan in E2 is not a vulnerability scan, and it is not counted here as one. A vulnerability scan would check for known weaknesses on a schedule, with findings handling and retesting. No such schedule, tool, or findings record is stated in this document. A buyer who needs vulnerability scanning should require it in writing for the relevant scope, with schedule, scope, and findings handling agreed before work starts. Until that commitment exists and is recorded, this answer stays not held, rather than borrowing the header scan grade to imply a wider testing position.

Related: Trust Center Security Practices section; E2; E4; E5.

F5. What backup schedule applies? [Answered to be confirmed in writing per engagement]

Answer: No backup schedule is stated in this document. The backup and recovery position for an engagement must be confirmed in writing per engagement.

Evidence: No backup schedule record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Two scopes must be kept apart. For the public site, source in GitHub supports a rebuild from source under F1, but no backup schedule, backup location, or restore timetable is claimed from that pattern alone. For engagement material, backup depends on the tools and the written

terms for that engagement, including how long a working copy is kept and how it is removed at engagement end under B5. No schedule in days, no retention figure for backups, and no restore time is given here, because none is verified in the evidence stated in this document. A buyer who needs a backup commitment should set it in writing for that engagement, before material is shared.

Related: Trust Center Documents section; B5; F1; K2; K3.

Category G: Incident response

G1. Is there a formal, published incident response plan? [Answered not held]

Answer: No formal, published incident response plan is claimed in this document.

Evidence: No incident response plan record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Evidence for this answer is limited to the items stated below. The contact route in G2 and the per-engagement notification timing in G3 are stated, but they are not presented as a full plan. A full plan would name roles, escalation steps, containment steps, communication steps, and post-incident review. None of those plan elements is stated generally here. A buyer who needs a plan should require it in writing for the relevant engagement, with roles and steps agreed before work starts, rather than treating the contact route alone as a plan.

Related: Trust Center Security Practices section; G2; G3; G5.

G2. What is the incident contact route? [Answered with evidence]

Answer: mohammad@movahedi.ca.

Evidence: Contact record in this document, dated Oct 27, 2026.

Detail: The same route given in A3 is the incident route, so a buyer does not need a second address for incidents. The route is stated, but the notification timing is not stated generally, and it is covered separately in G3 as a per-engagement confirmation. Keeping route and timing separate matters: a route that exists is evidenced, while a timing commitment that depends on the engagement is not overstated as a general service level figure.

Related: Trust Center Security Practices section; A3; G1; G3.

G3. How quickly will a client be notified of an incident affecting its material?

[Answered to be confirmed in writing per engagement]

Answer: No notification timetable is stated generally in this document. The timetable for an engagement must be confirmed in writing per engagement.

Evidence: No notification timetable record is stated in the evidence stated in this document, dated Oct 27, 2026. Contact route is given in G2.

Detail: Notification timing is a legal and contractual commitment, and it can carry regulatory consequences depending on the data and the jurisdiction involved. For that reason, a general figure in hours is not stated here without a source and without an engagement scope. A buyer should set the timetable in writing for that engagement, before material is shared, including what counts as a notifiable incident, who is notified, and by which route. The route in G2 then carries that notification, but the timetable itself comes from the written engagement terms.

Related: Trust Center Security Practices section; G2; B4; I4; L5.

G4. Has the vendor had a security incident affecting client material in the past 12 months? [Answered not held]

Answer: No incident history claim is made in this document.

Evidence: No incident history record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: This answer does not state that no incident ever occurred, and it does not state that an incident did occur. It states that no history claim is made here, so a buyer does not rely on a history statement with no source. A buyer who needs a history statement for a specific period should ask for it as a tailored response, using the route in Section 16, with the period and the scope stated in the request. That tailored answer can then be checked against its own date and scope, rather than read as a general claim in this questionnaire.

Related: Trust Center Documents section; G1; G2; Section 16.

G5. Has incident response been tested through a simulation or tabletop exercise? [Answered not held]

Answer: No simulation or exercise claim is made in this document.

Evidence: No testing record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Testing a plan and having a contact route are different things. G2 gives a route, G1 states

that no formal published plan is claimed, and this answer adds that no test of such a plan is claimed either. A buyer who needs a tested plan should require the test, with date, scope, and lessons, in writing for the relevant engagement. Until that record exists, this answer stays not held, and no exercise date is invented to fill it.

Related: Trust Center Security Practices section; G1; G2; K4.

Category H: Compliance, certifications, insurance, and clearance

H1. Does the company hold SOC 2? [Answered not held]

Answer: No. The company holds no SOC 2 certification.

Evidence: Company certification record in this document, dated Oct 27, 2026.

Detail: The answer is a plain no, with no qualifier and no implied equivalent. No SOC 2 report, report period, auditor name, or scope is claimed, because none exists in the record in this document. A buyer who needs SOC 2 assurance should not treat any other item in this document, including the header scan in E2 or the founder credentials in H4, as a substitute for SOC 2. Those items are different, and they are labelled as different.

Related: Trust Center Documents section; H2; H3; H4; H5.

H2. Does the company hold ISO 27001? [Answered not held]

Answer: No. The company holds no ISO 27001 certification.

Evidence: Company certification record in this document, dated Oct 27, 2026.

Detail: The answer is a plain no. No ISO 27001 certificate, scope statement, certification body, or validity date is claimed. The founder credentials in H4 are personal credentials, not a company ISO 27001 certification, and they are not presented as one. A buyer who needs ISO 27001 assurance should require a certificate and scope that can be checked, and this document does not offer one.

Related: Trust Center Documents section; H1; H3; H4.

H3. Does the company hold ISO 42001 or any other company certification? [Answered not held]

Answer: No. The company holds no ISO 42001 certification and no other company certification.

Evidence: Company certification record in this document, dated Oct 27, 2026.

Detail: This answer covers the remainder of the company certification question, so a buyer does not need to ask it a second time for another standard. The scope is company certifications, not personal credentials and not registrations. Registrations in A5 are registrations, and founder credentials in H4 are personal, and neither is counted as a company certification here. If a company certification is gained in future, it should be added as a new dated entry with its scope and validity date, under the improvement plan in Section 17, not backdated into this answer.

Related: Trust Center Documents section; A5; H1; H2; H4.

H4. What credentials does the founder hold? [Answered with evidence]

Answer: The founder holds ISC2 CC, CIPP/C, and Six Sigma Black Belt. These are personal credentials only.

Evidence: Personal credentials record in this document, dated Oct 27, 2026. The date of each credential is not stated in this document.

Detail: Each credential is named, and the personal-only limit is stated in the same answer, so the credentials cannot be misread as company certifications. ISC2 CC and CIPP/C are relevant to security and privacy work, and Six Sigma Black Belt is relevant to process work, but relevance is not the same as a company certification, an audit, or a client outcome. No credential number or issuer detail beyond the credential name is added here, because none is stated in the evidence stated in this document. A buyer who needs credential verification should ask for it as a tailored response, using the route in Section 16.

Related: Trust Center Documents section; A4; H1; H2; H3; L1.

H5. Does the company hold insurance? [Answered not held]

Answer: No insurance is held or claimed in this document.

Evidence: No insurance record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: No policy type, insurer, limit, or validity period is stated, because none is held or claimed in the record in this document. This matters for procurement: a buyer who needs insurance, for example professional liability or cyber cover, must require it in writing per engagement, before work starts, with the type and limit named in the written terms. Until such a requirement is met and recorded, a buyer should not assume cover exists. Clearance is covered separately in L4, where the same plain position applies.

Related: Trust Center Documents section; L4; L5.

Category I: Privacy and regulation

Legal scope note for this category: The services below are advisory services. They help a client understand and meet its own obligations. They are not certifications, they are not client outcomes, and they do not give legal advice for a specific client matter. A client's own legal position for a specific matter must be confirmed in writing per engagement, with the client's own counsel where the client needs it.

I1. What Law 25 compliance support is offered? [Answered with evidence]

Answer: Law 25 compliance support is offered as an advisory service.

Evidence: Service record in this document, dated Oct 27, 2026. Site in scope: https://movahedi.ca

Detail: Law 25 here means Quebec's privacy law reform work, approached as a compliance support service: mapping obligations, reviewing practices and materials, and helping a client plan its compliance steps. The service is the support, not a Law 25 certification, because no such company certification is claimed in H3. No client outcome under Law 25 is claimed from listing the service, and no client name is attached to it. The scope, the materials reviewed, and the deliverable for a specific client must be confirmed in writing per engagement, before work starts, so the client knows what the support covers and what it does not cover.

Related: Trust Center Documents section; A2; I4; L5.

I2. What EU AI Act readiness work is offered? [Answered with evidence]

Answer: EU AI Act readiness assessments are offered as an advisory service.

Evidence: Service record in this document, dated Oct 27, 2026. Site in scope: https://movahedi.ca

Detail: Readiness assessment means assessing how ready a client's AI use is against EU AI Act expectations, as an advisory exercise. It is not an EU AI Act certification, it is not a conformity assessment by a notified body, and it is not a client outcome. No client outcome under the EU AI Act is claimed from listing the service, and no client name is attached to it. The pattern of the work is inventory and risk analysis: listing AI and agent uses, mapping them to risk and governance expectations, and producing a readiness assessment with gaps and next steps. That pattern is stated in general terms only. The scope and the deliverable for a specific client must be confirmed in writing per engagement, before work starts.

Related: Trust Center Documents section; A2; I1; I4; J2.

I3. What privacy policy governs the public site? [Answered with evidence]

Answer: The Privacy Policy for movahedi.ca, last updated July 15, 2026.

Evidence: Privacy Policy record, last updated July 15, 2026. Site: https://movahedi.ca

Detail: The policy date is the evidence, and it is not moved forward to match this questionnaire. A buyer reading this questionnaire on Oct 27-28, 2026 therefore sees a policy dated July 15, 2026, which is the correct dated position. The policy governs the public site, not engagement material, which is governed by the engagement rules in Category B and the written terms for that engagement. If the policy is updated, the new date should be recorded as a new dated entry under the improvement plan in Section 17, with the old date kept in the change record, not overwritten without trace.

Related: Trust Center Privacy Policy section; Trust Center Documents section; B1; B2; I4.

I4. Does the vendor claim general compliance with privacy laws such as PIPEDA or GDPR? [Answered to be confirmed in writing per engagement]

Answer: No general compliance claim is made in this document. The compliance position for a specific engagement must be confirmed in writing per engagement.

Evidence: No general compliance claim record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Privacy compliance depends on the data, the purpose, the jurisdiction, and the roles of the parties in a specific engagement. A blanket claim covering every law and every engagement would hide those variables, so none is made. Instead, the services in I1 and I2 are offered as support and assessment, the client data rules in Category B set the default handling position, and the specific compliance position, including roles, lawful basis or authority where relevant, transfer rules, and notification duties, must be set in writing for that engagement, before material is shared. This document is company information, not legal advice for a specific client matter, and a client that needs a legal position for its own matter should confirm it with its own counsel as part of that written confirmation.

Related: Trust Center Privacy Policy section; B4; G3; I1; I2; L5.

I5. Are client materials sold, used for training, or named publicly? [Answered

with evidence]

Answer: No. Client material is not sold, it is not used for model training, and no client is named publicly without written permission.

Evidence: Client data rules record in this document, dated Oct 27, 2026.

Detail: Three separate prohibitions are stated, and each stands on its own. No sale covers transfer for value to an unrelated party. No model training use covers the vendor's own models and third party models alike. No public naming without written permission covers case studies, client lists, logos, testimonials, and any other public naming. Written permission is the only exception stated for public naming, and it must be permission for that specific naming, not a general engagement signature read as naming consent. No client is named anywhere in this document, and no testimonial or logo is included, consistent with this rule.

Related: Trust Center Documents section; B2; B5; J5; L5.

Category J: Subprocessors and third parties

J1. Which third parties deliver the public site? [Answered with evidence]

Answer: GitHub for source and deployment, and Cloudflare for delivery over HTTPS.

Evidence: Technology record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: These two providers are the delivery chain for the public site, and they are named because a buyer assessing the site needs to know the chain. No other delivery provider is claimed for the public site. No plan tier is claimed for either provider, as stated in D2. No client data sits on the public site under B1, so the delivery chain for the public site is not a client data processing chain. Engagement tools are a separate matter and are covered in J2, where per-engagement confirmation applies.

Related: Trust Center Security Practices section; D1; D2; F1; J2.

J2. Which third parties will handle client engagement material? [Answered to be confirmed in writing per engagement]

Answer: No engagement third party list is stated generally in this document. Any third party that will handle engagement material must be confirmed in writing per engagement.

Evidence: No engagement third party list is stated in the evidence stated in this document, dated

Oct 27, 2026.

Detail: Engagement tools can vary by engagement: a shared folder, a review tool, a research source, or a delivery channel agreed for that engagement. Because the list varies, a general list stated here would be wrong for at least some engagements. The correct position is a per-engagement list, agreed in writing before material is shared, naming each third party, what it will handle, and for what purpose. If no third party will handle the material, that too should be stated in the written terms for that engagement, so the absence is recorded rather than assumed.

Related: Trust Center Documents section; B2; C1; D3; J3; J5.

J3. How will a client be told about a change to an engagement third party? [Answered to be confirmed in writing per engagement]

Answer: No change notice rule is stated generally in this document. The notice rule for an engagement must be confirmed in writing per engagement.

Evidence: No change notice record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: A change to a third party can change risk, residency, or access, so a buyer needs to know in advance how a change will be communicated and whether approval is needed before the change takes effect. That rule depends on the engagement, so it belongs in the written terms for that engagement, before work starts. The written rule should cover what counts as a change, how notice is given, how much notice is given, and whether the client can object. No notice period in days is stated here, because none is verified generally in the evidence stated in this document.

Related: Trust Center Documents section; J2; J5; L5.

J4. Is there a published vendor assessment process for third parties? [Answered not held]

Answer: No published vendor assessment process is claimed in this document.

Evidence: No vendor assessment process record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Evidence for this answer is limited to the items stated below. The delivery providers for the public site are named in J1, and engagement third parties are confirmed per engagement in J2, but a documented assessment process, with criteria, review steps, and records, is not claimed. A buyer who needs such a process should require it in writing for the relevant scope, with criteria

and records agreed before a third party handles material. Until that process exists and is recorded, this answer stays not held.

Related: Trust Center Security Practices section; J1; J2; J3.

J5. Is client material shared with third parties beyond the engagement? [Answered with evidence]

Answer: No. Client material is used only for its engagement, it is not sold, and it is not shared for an unrelated purpose.

Evidence: Client data rules record in this document, dated Oct 27, 2026.

Detail: This answer restates the B2 use limit from the sharing angle, so a buyer reading only this category still gets the limit. Sharing within an engagement, to a third party agreed in writing under J2, is different from sharing beyond the engagement, and only the first is possible under this rule, and only where the written terms allow it. Sharing beyond the engagement, for marketing, for another client, for sale, or for training, is not allowed under B2 and I5. No third party beyond the engagement is named as a recipient anywhere in this document.

Related: Trust Center Documents section; B2; I5; J2; J3.

Category K: Business continuity and availability

K1. What uptime service level is offered for movahedi.ca or for engagement work? [Answered not held]

Answer: No uptime service level is claimed in this document.

Evidence: No service level record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: No percentage, no measurement period, and no credit or remedy is stated, because none is held or claimed in the record in this document. The public site is live, as stated in K5, but live today is not an uptime promise for tomorrow, and it is not presented as one. A buyer who needs an availability commitment for a specific service or engagement must require it in writing, with the service, the measurement, and the remedy named, before work starts. Until that commitment exists, this answer stays not held.

Related: Trust Center Documents section; E5; K5; L5.

K2. What recovery time and recovery point objectives apply? [Answered to be confirmed in writing per engagement]

Answer: No recovery time objective and no recovery point objective is stated in this document. Both must be confirmed in writing per engagement where they are needed.

Evidence: No recovery objective record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Recovery objectives are numbers with consequences: a time to restore, and a point in time to restore to. Stating them generally, without a service scope and without a tested recovery record, would give a buyer numbers with no way to check them. For the public site, the rebuild-from-source pattern in F1 is stated, but no time objective is drawn from it. For engagement material, recovery depends on the tools and terms for that engagement, and any objective must be agreed in writing for that engagement, before material is shared.

Related: Trust Center Documents section; F1; F5; K3; K4.

K3. Is there a formal business continuity plan? [Answered not held]

Answer: No formal business continuity plan is claimed in this document.

Evidence: No business continuity plan record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Evidence for this answer is limited to the items stated below. The public site rebuild pattern in F1 and the engagement removal rule in B5 are stated, but neither is presented as a formal business continuity plan. A formal plan would name continuity risks, alternate arrangements, roles, and review steps. None of those plan elements is stated generally here. A buyer who needs a plan should require it in writing for the relevant scope, before work starts, rather than treating the rebuild pattern alone as a plan.

Related: Trust Center Documents section; F1; K2; K4.

K4. Has disaster recovery been tested? [Answered not held]

Answer: No disaster recovery test is claimed in this document.

Evidence: No recovery test record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Testing recovery and being able to rebuild from source are different things, and the answer

keeps them separate. F1 states the rebuild pattern for the public site. This answer adds that no test date, test scope, test result, or retest record is claimed for disaster recovery. A buyer who needs a tested recovery position should require the test in writing, with date, scope, and result, for the relevant scope. Until that record exists, this answer stays not held, and no test date is invented to fill it.

Related: Trust Center Documents section; F1; F5; K2; K3; G5.

K5. Is movahedi.ca currently live? [Answered with evidence]

Answer: Yes. The site is a live public site, as recorded in this document on Oct 27-28, 2026.

Evidence: Site record in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: Live status is stated as a dated observation, not as an availability promise. It means a buyer can check the site at the link given and see the public site that this questionnaire describes. It does not carry an uptime figure, a service level figure, or a future availability promise, and none is added here, consistent with K1. If the site moves, changes provider, or changes scope, the dated record should be updated under the improvement plan in Section 17, with the change dated, not silently overwritten.

Related: Trust Center Documents section; D1; E1; E2; K1.

Category L: People, physical security, and contract terms

L1. What screening applies to people who will access client material? [Answered not held]

Answer: No screening claim is made in this document.

Evidence: No screening record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Screening is a specific commitment: a check type, a scope, and a point in time. No check type is stated here, because none is verified in the evidence stated in this document. Personal credentials in H4 are credentials, not screening checks, and they are not presented as screening. A buyer who needs screening, for example a background check or a reference check for people who will access its material, must require it in writing per engagement, before access is granted, naming the check and the people it covers. That written requirement is where A4, C1, and this answer meet: staffing, access, and screening are confirmed together, before work starts.

Related: Trust Center Documents section; A4; C1; H4; L5.

L2. What security training is given to staff? [Answered not held]

Answer: No security training claim is made in this document.

Evidence: No training record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: Evidence for this answer is limited to the items stated below. Personal credentials in H4 show personal qualifications, but they are not a staff training programme, and they are not presented as one. No training topic, frequency, attendance record, or completion rate is stated, because none is verified in the evidence stated in this document. A buyer who needs training for people who will work on its engagement should require it in writing per engagement, naming the training and the people it covers, before work starts.

Related: Trust Center Documents section; A4; H4; L1.

L3. What physical security applies to a vendor facility holding client data? [Answered not applicable]

Answer: No facility physical security claim applies, because no vendor facility holding client data is claimed.

Evidence: Site and service scope records in this document, dated Oct 27-28, 2026. Site: https://movahedi.ca

Detail: Physical security questions assume a facility, a data centre, or an office store holding client records. That model does not fit this vendor: the public site holds no client data under B1, engagement work is advisory, and no data centre or client data store facility is claimed. A buyer assessing physical security for a hosted data store should not use this answer, because no such store is claimed. Engagement material protection is covered instead by the use limits in Category B, the access limits in Category C, and the per-engagement confirmations in this document.

Related: Trust Center Security Practices section; B1; D5; J1.

L4. Does the vendor hold a security clearance? [Answered not held]

Answer: No. No security clearance is held or claimed in this document.

Evidence: No clearance record is stated in the evidence stated in this document, dated Oct 27, 2026.

Detail: The answer is a plain no, with no level, no issuing body, and no validity date added, because none exists in the record in this document. Registrations in A5 are registrations, not clearances, and they are not presented as clearances. Personal credentials in H4 are personal credentials, not clearances, and they are not presented as clearances. A buyer who needs a clearance for specific work must require it in writing per engagement, before work starts, naming the level and the people it must cover. Until such a requirement is met and recorded, a buyer should not assume clearance exists.

Related: Trust Center Documents section; A5; H4; H5; L5.

L5. How are specific security, screening, or insurance requirements agreed for an engagement? [Answered with evidence]

Answer: They are confirmed in writing per engagement, before work starts, using the contact route mohammad@movahedi.ca.

Evidence: Contract route record in this document, dated Oct 27, 2026. Contact: mohammad@movahedi.ca

Detail: This answer is the closing rule for the whole questionnaire, and it is stated as evidence because the route and the timing rule are both stated generally in this document. Specific security requirements, screening requirements, and insurance requirements are not general claims in this questionnaire: security requirements that depend on an engagement are in C2, C3, C4, D3, and F2; screening is in L1; insurance is in H5; clearance is in L4. Each of those answers points to this written confirmation step. The confirmation must name the requirement, the scope, and the people or material it covers, so it can be checked after work starts. A requirement that is not confirmed in writing for that engagement should not be assumed to apply to that engagement.

Related: Trust Center Documents section; A3; B3; B4; C2; H5; L1; L4; Section 16.

15. Cross-link index

The cross-links used in this questionnaire are listed below by thread, so a buyer can follow any thread to its evidence and back. A cross-link name is a section or document name to check, not a second claim. Where a live link exists, it is the site link or the scan link given in the evidence paragraphs. No other URL is invented in this index.

- Company thread: Category A, Trust Center Documents section, Trust Center Security Questionnaire Answers section, Trust Center Registrations section, H4, L5.
- Public site thread: Section 2.1, Section 2.2, D1, E1, E2, E3, K5, site https://movahedi.ca, scan

https://securityheaders.com/?q=https://movahedi.ca&followRedirects=on

- Header scan thread: Section 2.2, E1, E2, E3, E4, F4, Trust Center Security Practices section, Trust Center Documents section.
- Privacy Policy thread: Section 2.3, I3, B1, B2, I4, Trust Center Privacy Policy section, Trust Center Documents section.
- Client data thread: Category B, Category C, I5, J2, J5, L1, Trust Center Documents section, Trust Center Privacy Policy section.
- Access thread: Category C, B5, J2, L1, Trust Center Security Practices section.
- Infrastructure thread: Category D, F1, J1, K5, Trust Center Security Practices section.
- Testing limits thread: E4, F4, G5, K4, Trust Center Security Practices section. Each of these answers states what is not held, so the limits thread is as checkable as the evidence thread.
- Certification limits thread: H1, H2, H3, H5, L4, A5, H4. Registrations and personal credentials are kept separate from company certifications in this thread.
- Privacy and regulation thread: Category I, Category B, G3, Trust Center Privacy Policy section, Trust Center Documents section.
- Third party thread: Category J, D1, D2, B4, Trust Center Security Practices section, Trust Center Registrations section.
- Continuity thread: Category K, F1, F5, B5, Trust Center Documents section.
- Contract thread: L5, Section 16, A3, G2, and every answer marked to be confirmed in writing per engagement: A4, B3, B4, C2, C3, C4, D3, D4, F2, F5, G3, I4, J2, J3, K2.
- Registration thread, one entry at a time: Section 2.4 UNGM Basic 1295964, Section 2.5 MERX Basic Free, Section 2.6 CanadaBuys and SAP Ariba AN11542201146, Section 2.7 CPSS ePortal, Section 2.8 Ontario Tenders Portal, Section 2.9 LinkedIn Services, Section 2.10 Catalant, Section 2.11 Clutch 0 reviews, Section 2.12 Trustpilot 0 reviews and 0.0, all dated Oct 27, 2026, plus A5.
- Personal credentials thread: Section 2.13, H4, A4, L1, L2, L4.
- Version thread: Section 2.14, Section 1, Trust Center Documents section, Trust Center Security Questionnaire Answers section. Trust Center v1, v2, v3, and v4 all fall on Oct 27, 2026.

16. Request route for a tailored response

To request a tailored response to a specific questionnaire, a fresh confirmation for a single entry, or written confirmation for a specific engagement, contact mohammad@movahedi.ca.

In the request, state:

1. The question number from this questionnaire, for example B3, G3, or J2, or the new question in full.
2. The engagement scope the question covers, where it covers an engagement.

3. The specific commitment needed, for example a retention period, a notification timetable, a screening check, an insurance type and limit, or a clearance level.
4. The date by which a written confirmation is needed, where a date applies.

A tailored response will be given as a dated, written confirmation for that request. It will not change the general answers in this questionnaire by implication. If a tailored confirmation differs from a general answer for a specific engagement, the tailored written confirmation governs that engagement, and the change will be recorded as a dated entry under the improvement plan in Section 17.

17. Improvement note: review, refresh, and addition over the next year

This note is a proposed improvement plan. It is not a completed routine, and no routine starts from this note alone. A cadence is adopted only when it is approved.

Purpose: Keep this questionnaire true as evidence changes, without backdating, without silently overwriting an old answer, and without adding a claim before its evidence exists.

Stage 1, monthly evidence re-checks:

- Re-check the live site at https://movahedi.ca and re-run the header scan at https://securityheaders.com/?q=https://movahedi.ca&followRedirects=on
- Compare the new scan grade, date, and header list to E2 and E3. If anything changed, add a new dated entry and update E2 and E3 with the new date, keeping the old dated result in the change record.
- Re-check the Privacy Policy date. If the policy date moved from July 15, 2026, update I3 and Section 2.3 with the new date, keeping the old date in the change record.
- If a monthly re-check finds no change, record that fact as a dated check with no change, rather than leaving the month blank.

Stage 2, quarterly VSQ and registrations refresh:

- Once each quarter, review every answer in Categories A to L against fresh evidence, and review every registration and third-party profile in Section 2.4 to Section 2.12 and in A5.
- For each registration and profile, confirm whether it is still held, whether its identifier changed, and whether its review count changed, for example Clutch and Trustpilot counts. Update each entry on its own, with its own new date, not as a shared row.
- Review every answer marked not held. If an item has since been gained, for example a company certification, an insurance policy, a clearance, a formal incident response plan, or a

penetration test, add it as a new dated entry with its scope and validity date, and change that answer from not held to answered with evidence, with the change dated. Do not backdate the gain to Oct 27, 2026.

- Review every answer marked to be confirmed in writing per engagement. If a general company position has since been set, for example a standard retention period or a standard notification timetable, record it as a new dated general position only where it truly applies generally. Otherwise, keep the answer as per-engagement confirmation.
- Review the Trust Center Documents section and the Security Questionnaire Answers section links for this questionnaire, so the published questionnaire matches the current version in this file.

Stage 3, dated log entry for every change:

- Every change, however small, gets a dated log entry stating what changed, when it changed, and what evidence supports the change. The Trust Center Updates section shows a clean, dated summary, with what changed and when.
- No change is made by silently editing an old date. An old date stays as the record of the old position, and a new date records the new position.
- If a change corrects an error in this questionnaire, the correction states what was wrong and what the correct position is, in the same dated entry.

Stage 4, annual review at the end of the year:

- At the end of the year covered by this plan, review the whole questionnaire, the evidence index, and the cross-link index together, and confirm that every count in the summary still matches the answers, that every link still resolves to the source named, and that every not held answer is still honestly not held.
- Produce a new dated version only where a change in evidence supports it. If no evidence changed, record the annual review as a dated check with no change, rather than issuing a new version for its own sake.

Approval required: the monthly, quarterly, and annual cadence above, and the dated entry rule, before any routine starts. No routine starts from this note alone.