traztech

Cybersecurity & Compliance Consulting

Security Assessment Attestation

Specimen document

Kestrel Data Systems Inc.

Prepared for	Kestrel Data Systems Inc.
Prepared by	Jacob Masse, Principal, TrazTech Inc.
Date	April 9, 2026
Reference	PT-2026-03

Specimen document

This is a published example of the attestation letter TrazTech issues after a security engagement. It is not a record of any engagement and it attests to nothing. The client, the systems, the findings, the dates and the signature below are invented for illustration. Every page carries a specimen mark.

9 April 2026

To whom it may concern

Subject: Kestrel Data Systems Inc. security assessment

TrazTech Inc. was engaged by Kestrel Data Systems Inc. to perform the security testing described below. This letter is issued at the request of Kestrel Data Systems Inc. so that it may be shared with customers, insurers and other third parties who ask about the state of its security programme.

What we assessed

TESTING TYPE	**Grey box penetration test, credentialed and unauthenticated**
TARGETS	**app.kestreldata.invalid (production web application and REST API) and admin.kestreldata.invalid (administrative console)**
TESTING WINDOW	**2 to 9 March 2026**
RETEST WINDOW	**24 March 2026**
FRAMEWORK OF REFERENCE	**OWASP Testing Guide and the Penetration Testing Execution Standard**

Systems and environments not named above were outside the scope of this engagement and were not tested.

What we did

Testing was performed manually by a named tester, supported by automated tooling for the discovery of known patterns. Coverage spanned authentication, session management, authorisation across three role levels, input validation, business logic, file handling, the documented API surface, transport configuration and the client side.

Confirmed conditions were exploited only so far as was necessary to establish impact and assign severity. No destructive testing was performed, and no production data was extracted beyond what was required to evidence a finding.

What we observed

Nine findings were raised: one critical, two high, three medium, two low and one informational. The critical finding concerned authorisation on a record-retrieval endpoint. The two high findings concerned multi-factor coverage on an administrative interface and session invalidation on credential change.

Seven of the nine findings, including the critical finding and both high findings, were remediated by Kestrel Data Systems Inc. and independently verified by TrazTech on retest on 24 March 2026. The two findings that remain open are rated low and informational respectively, and neither presents a material risk to customer data in the environment as tested.

No evidence was found of prior unauthorised access, and no customer data was found to have been exposed as a consequence of any finding in this engagement.

The limits of this letter

This letter is a statement of the work TrazTech performed and what we observed while performing it. It is not an audit opinion, it is not a certification, and it does not carry the assurance of an accredited attestation. Only a licensed audit firm can issue one of those, and nothing in this letter should be read as one.

Our observations relate to the scope and the dates stated above. Security posture changes. A control that operated correctly during the testing window may not operate correctly today, and a subsequent deployment can reintroduce a finding recorded here as closed.

This letter is provided for information. TrazTech accepts no liability to any third party who relies on it.

Contact

Questions about the work described here can be directed to Jacob Masse at TrazTech Inc., hello@traztech.ca, quoting reference PT-2026-03.

Jacob Masse
Principal, TrazTech Inc.
hello@traztech.ca | traztech.ca

SIGNED

Jacob Masse

Jacob Masse, Principal
TrazTech Inc.

Signed 9 April 2026 · Reference PT-2026-03