LEGAL AGREEMENT

CONFIDENTIALITY AND AUTHORIZED SECURITY TESTING AGREEMENT

EMP-2024-UK-001

January 1, 2026 • December 31, 2028

CONTRACTING PARTIES

FIRST PARTY

Tech Innovations Ltd

45 Queen Street
London
EC1V 9DS
United Kingdom

contact@techinnovations.co.uk | +44 20 7946 0123

SECOND PARTY

John Smith

78 Baker Street
London
NW1 6XE
United Kingdom

john.smith@email.com | +44 7712 345678

TERMS AND CONDITIONS

1. Definition of Confidential Information

For purposes of this Agreement, **“Confidential Information”** includes any non-public information disclosed or accessed by the Security Consultant in connection with the Security Services, including but not limited to:

- network diagrams, system architecture, configurations
- source code, binaries, firmware, scripts, exploits, payloads
- credentials, authentication data, encryption keys, tokens
- vulnerability reports, penetration test results, risk ratings
- security controls, monitoring systems, incident data
- customer data, logs, backups, and personally identifiable information (PII)

Confidential Information may be written, electronic, oral, or observed during testing activities.

---

2. Authorized Access and Scope Acknowledgment

The Client acknowledges that the Security Consultant is **explicitly authorized** to perform testing activities **only within the approved scope** defined in a separate statement of work, engagement letter, or written authorization.

Any access, exploitation, or testing performed **outside the agreed scope** is expressly prohibited.

---

3. Exclusions from Confidential Information

Confidential Information does **not** include information that the Security Consultant can demonstrate:

a. is publicly available through lawful means;
b. was lawfully known prior to disclosure by the Client;
c. is independently developed without reference to Client systems or data;
d. is lawfully obtained from a third party without breach of obligation;
e. is disclosed with the Client’s prior written consent.

---

4. Obligations of the Security Consultant

The Security Consultant agrees to:

a. use Confidential Information solely for performing authorized Security Services;
b. not disclose vulnerabilities, findings, or sensitive details to any third party without written Client approval;
c. store all Confidential Information using reasonable and appropriate technical and organizational security measures;
d. immediately notify the Client of any critical vulnerabilities, data exposure, or system compromise discovered during testing;
e. avoid intentional service disruption, data destruction, or persistence mechanisms unless explicitly authorized in writing.

---

5. Reporting and Vulnerability Disclosure

All vulnerability findings, exploit details, and risk assessments shall be reported exclusively to the Client.

Public disclosure, publication, conference talks, blog posts, or proof-of-concept sharing related to the Client's systems require **prior written consent** from the Client.

---

6. Data Handling and Retention

Upon completion or termination of the engagement, the Security Consultant shall, upon request:

- securely delete or return all Client data, reports, credentials, and artifacts;
- certify in writing that all Confidential Information has been destroyed, except where retention is required by law.

---

7. Term and Survival

This Agreement shall remain in effect during the term of the Security Services.

Confidentiality obligations shall survive termination and continue until the Confidential Information becomes publicly available through lawful means or the Client provides written release.

---

8. Intellectual Property

All reports, findings, and deliverables created under this Agreement shall be the property of the Client, unless otherwise agreed in writing.

Nothing in this Agreement grants the Security Consultant ownership of Client systems, data, or intellectual property.

---

9. Independent Contractor Status

The Security Consultant is an independent contractor. Nothing in this Agreement creates an employment, partnership, joint venture, or agency relationship.

---

10. Whistleblower and Legal Disclosure Immunity

Nothing in this Agreement prohibits disclosure of Confidential Information to government authorities or legal counsel for the purpose of reporting a suspected violation of law, provided such disclosure complies with applicable whistleblower protection laws.

---

11. Severability

If any provision of this Agreement is found unenforceable, the remaining provisions shall remain in full force and effect.

---

12. Entire Agreement

This Agreement constitutes the entire understanding between the Parties regarding confidentiality and authorized security testing and supersedes all prior discussions or agreements relating to such matters.

---

13. Binding Effect

This Agreement shall be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns.

SPECIAL PROVISIONS

None

EXECUTED AGREEMENT

PARTY A

Jane Doe

HR Director

January 1, 2026

PARTY B

John Smith

Employee

January 1, 2026

WITNESS

Emily Clark

SEAL

NOTARY PUBLIC ATTESTATION

SEAL

Notary Public Registration No. 123456