Service Definition Document (Accessible Version

Service Name: Penetration Testing and Vulnerability Assessment Certification
Supplier: Indelible Data Limited
Service Type: Cyber Security Assurance

---

1. Service Description

Indelible Data Limited provides Penetration Testing and Vulnerability Assessment services.
We help organisations check their IT systems against UK Government cyber security standards.

Comprehensive security assessments of Cloud and infrastructure environments, ranging from automated vulnerability scanning to advanced manual adversary simulation.

Our service:

- **Public, Private, and Hybrid cloud configurations on GCP.**
- **All testing follows UK NCSC CHECK standard and penetration testing methodology.**
- **Reduces cyber risk**
- **Helps organisations run cloud and digital services securely**

---

2. Service Features

- **Targeted Cloud Testing: Specialised testing**
- **Web Application Penetration Test: Assessment of OWASP Top 10 risks.**
- **Infrastructure Penetration Test: Internal and external vulnerability scanning and exploitation.**
- **Configuration Review.**
- **Mobile App Penetration Testing**

- **Alignment with NCSC guidance and Cloud First principles**
- **Endpoint Penetration Test**
- **Minimal disruption to live services and operations**
- **Remediation Support Post-test debriefs and retesting to verify fixes.**
- **Endpoint Penetration Test**

---

3. Service Benefits

- **Penetration Testing Reduces risk of common cyber threats and attacks**
- **Penetration test will build confidence with stakeholders and partners**
- **Penetration Test supports secure adoption of cloud services**
- **Penetration Test will enhance organisational cyber resilience and governance**
- **Provides practical, actionable guidance for ongoing improvement**
- **Align with NCSC guidelines and Cyber Essentials Plus requirements.**
- **Identify and mitigate critical entry points before attackers exploit them.**
- **Penetration Test Delivered by Cyber Scheme Team Member or Leader**
- **Align to compliance standards DCC, GDPR, PCIDSS, ISO27001**
- **Penetration Test will identify weaknesses in your systems**

---

4. Service Constraints

Notice Periods: A requirement for a minimum notice period before testing can commence to ensure resource availability.

---

5. Support Levels

A comprehensive security assessment involving manual Penetration Testing and exploitation techniques to uncover complex, chained vulnerabilities within specific cloud-native environments.

Scope: Includes authenticated and unauthenticated testing to simulate different attacker profiles.

Deliverables: A detailed technical report featuring an executive summary, proof-of-concept for findings, and tactical remediation steps.

Support: Dedicated account manager and a post-test debrief session via telephone or video call to discuss findings and remediation roadmaps.

All support is provided during UK working hours, with options for extended or bespoke support agreed at contract stage.

---

6. Service Deliverables

Pre-Engagement Deliverables

- **Rules of Engagement (RoE): A formal document outlining the testing window, authorized IP ranges, emergency contact details.**
- **Scoping Document: A signed agreement defining the specific GCP Project IDs, VPCs, and APIs in scope to prevent "scope creep" and accidental testing of out-of-scope assets.**

Technical Deliverables (The Core Report)

- **Executive Summary: A non-technical overview for senior stakeholders outlining the overall security posture and business risk.**
- **Technical Findings Matrix: A detailed breakdown of vulnerabilities (e.g., OWASP Top 10), each containing:**
    - **CVSS v3.1/v4.0 Scoring: Standardised severity ratings.**
    - **Proof of Concept (PoC): Screenshots and logs demonstrating how the vulnerability was identified.**
    - **Remediation Guidance: Specific instructions for GCP**

Management & Compliance Deliverables

- **Risk Remediation Plan: A prioritised roadmap tailored for the buyer's technical team to track fix progress.**
- **Attestation of Remediation (Letter of Conformance): A summary document often used for third-party audits (e.g., proving security to the NCSC) confirming that a test was conducted and critical risks were addressed.**
- **Clean-up Log: Verification that all temporary testing accounts, SSH keys, and test data created during the engagement have been removed from the GCP environment.**

Post-Test Support

- **Debrief Presentation: A virtual or on-site session to walk technical teams through complex findings and answer remediation questions.**
- **Re-testing Report: (Optional/Level-dependent) A follow-up validation report confirming that specific vulnerabilities have been successfully mitigated.**