SAFEHARBOUR SECURITY

Service Definition Document

Penetration Testing

Service: Penetration Testing
Supplier: Safe Harbour Security
Date: January 2026

Version	Approved by
1.0	Gary O'Brien

Service Description Document

What is Penetration Testing

Safe Harbour Security provides an end-to-end penetration testing service designed to identify and validate security vulnerabilities across networks, systems, applications, APIs, cloud platforms, and supporting infrastructure. The service combines automated scanning with expert-led manual testing to assess real-world attack vectors and evaluate the effectiveness of existing security controls.

All testing is delivered using recognised industry-standard methodologies, including the Penetration Testing Execution Standard (PTES), the Open Source Security Testing Methodology Manual (OSSTMM), and the OWASP Testing Methodology.

Engagements are tailored to the organisation's risk profile, operational environment, regulatory obligations, and governance objectives. The scope, depth, and testing approach can be adapted to meet specific requirements, ensuring assessments are both proportionate and effective.

The objective of the service is to reduce the likelihood of exploitation, strengthen technical defences, and support regulatory, compliance, and internal assurance requirements through clear, risk-prioritised and actionable remediation guidance.

Business Continuity & Data Protection

Penetration testing does not involve hosting or managing customer production systems or operational data. However, Safe Harbour Security maintains secure processes for handling engagement-related information (evidence, notes, and reports).

Backup Levels

- Backups are retained only for the duration necessary to complete the engagement or to support agreed retesting.

Restore & Retention Policy

- Testing data is retained for 24 months.
- Sharepoint can recover deleted files within a 90 day window from when they were deleted.
- Reports are encrypted and held for 24 months unless otherwise agreed with the client.

Business Continuity & Disaster Recovery

- Safe Harbour Security maintains documented Business Continuity and Disaster Recovery plans in alignment with ISO/IEC 27001 requirements, designed to support service continuity and operational resilience.

In accordance with our Data Retention Policies and UK GDPR, our customer engagement data is never retained longer than necessary to support reporting and agreed exit processes.

Service Description Document

Service Features

Our services include but are not limited to:

- Vulnerability Scanning
- External & Internal Infrastructure Assessments
- Web Application Security Assessments
- API Security Assessments
- Mobile Application Security Assessments
- Cloud Configuration Assessments (Azure, AWS, GCP)
- Machine Build Reviews (Windows, Unix, Linux)
- Firewall Configuration Reviews
- Wireless Security Assessments
- VPN Security Assessments
- Source Code Security Review

Service Benefits

- Identifies vulnerabilities before adversaries can exploit them
- Reduces breach risks and uncovers misconfigurations
- Supports secure software deployment
- Protects sensitive customer and organisational data
- Reduces cloud exposure and enforces least-privilege principles
- Strengthens endpoint hardening and baseline configuration
- Ensures proper network segmentation and access control
- Protects wireless infrastructure through secure configuration
- Ensures strong authentication and encryption in VPN deployments
- Improves secure coding practices

Service Description Document

Onboarding

Before any penetration testing engagement begins, Safe Harbour Security works closely with clients to ensure a smooth, efficient, and well-prepared start. Our onboarding process establishes clear objectives, defines the scope of work, and ensures that all necessary access, approvals, and documentation are in place. This structured approach helps minimise risk and maximises the value delivered by the engagement.

Typical onboarding steps include:

- Initial scoping workshop
- Definition of rules of engagement
- Identification of in-scope assets and access requirements
- Agreement of testing schedules and communication channels
- Provisioning of test accounts and access (as required)
- Pre-engagement documentation and approvals

Off-boarding & Exit Support

At the conclusion of each engagement, Safe Harbour Security provides structured offboarding to ensure clients can effectively act on the findings and securely retain or remove engagement data. This process helps organisations integrate remediation into their ongoing security programme and ensures a clear end to the engagement.

Offboarding and exit support includes:

- Complete technical report with evidence and remediation steps
- Executive summary for management and governance audiences
- Post-engagement debrief session
- Support for remediation queries
- Optional retesting to validate fixes
- Secure data return or deletion, with confirmation upon request

Service Constraints

Safe Harbour Security delivers flexible testing services, but certain limitations and operational constraints must be considered to ensure safe, effective, and authorised testing. By clarifying these constraints upfront, clients can plan appropriately and avoid unintentional service disruption.

Typical service constraints include:

- Some tests may require out-of-hours or maintenance window scheduling
- Customer-provided credentials or test accounts may be required
- Cloud assessments are subject to provider logging and permission availability
- Customer approval is required for intrusive testing activities
- Source code reviews rely on customer-provided access

Service Description Document

Service Levels

Safe Harbour Security is committed to delivering penetration testing services that meet agreed standards of quality, responsiveness, and reliability. Service levels provide clients with a clear understanding of expected performance, reporting timelines, and incident escalation, helping them plan and manage security activities effectively.

- Testing Availability: As per agreed test schedule
- Support Hours: 09:00–17:00 Monday–Friday (UK time)
- Critical Issue Notification: Immediate escalation through designated contact
- Reporting: Draft report within 5-10 working days of test completion

After-Sales Support

Safe Harbour Security provides ongoing support after each engagement to ensure clients can understand, prioritise, and act on findings. After-sales support helps maximise the value of the penetration testing exercise and supports continuous improvement of the client's security posture.

- Follow-up sessions to review results
- Assistance with remediation prioritisation
- Clarification on reported findings
- Optional retesting of previously identified vulnerabilities
- Access to security specialists during support hours

Technical Requirements

To deliver effective and safe penetration testing services, Safe Harbour Security may require certain technical resources and access from the client. These requirements ensure that testing can be performed efficiently, securely, and with minimal impact on business operations.

Technical requirements may include:

- Credentialed access (for authenticated testing)
- IP allowlisting for Safe Harbour Security testing infrastructure
- Access to cloud consoles, dashboards or security tooling
- API documentation or schemas
- Architecture diagrams, network maps, or environment information
- Code access for source code review

Hosting Locations

Safe Harbour Security does not host customer systems.
All testing platforms and engagement data storage reside in secure environments located within the United Kingdom and EU.

Service Description Document

Outage & Maintenance Management

Safe Harbour Security acknowledges that penetration testing can have an impact on systems and applications. To minimise disruption and ensure testing is safe and controlled, we provide clear procedures for managing outages and maintenance events. This enables clients to plan activities around normal operations and ensures any unexpected events are handled appropriately.

- Testing activities may be suspended or deferred where system instability, degradation, or elevated operational risk is identified.
- Intrusive testing activities are conducted strictly within pre-agreed testing windows, as defined in the applicable Statement of Work and Terms and Conditions.
- The Client may request the temporary suspension of testing activities at any time, subject to reasonable notice.
- Any critical or high-severity issues identified during testing that present an immediate risk to system availability or security will be communicated to the Client without undue delay.

In accordance with the Terms and Conditions, the Client acknowledges that penetration testing is inherently intrusive and may result in temporary service disruption or reduced system availability. Safe Harbour Security shall use reasonable endeavours to minimise such impact but shall not be liable for outages or service degradation arising from the agreed scope of testing activities, except to the extent required by applicable law.

Data Access Upon Exit

Ownership:
Customers retain full and exclusive ownership of all deliverables produced during the engagement.

Customer Exit Rights:
Upon conclusion of services, customers may request:

- Copies of all reports and supporting evidence, up to 24 months following the completion of testing.
- Transfer of customer data in mutually agreed formats.
- Secure deletion of customer data, up to 24 months following the completion of testing unless otherwise agreed with the client.

Data Retention:

- Raw Testing Data, Credentials, and Evidence: Retained for a period of up to 90 days following delivery of the final report.
- Final Reports: Retained for up to 24 months for contractual, audit, and quality assurance purposes.

Compliance:
All data handling, retention, and deletion procedures are conducted in accordance with applicable laws and industry best practices.

Service Description Document

Security

Safe Harbour Security applies robust security controls to protect client information, testing environments, and engagement data throughout the lifecycle of the penetration testing engagement. These measures ensure that all findings, evidence, and reports are handled securely, maintain confidentiality, and comply with recognised industry standards.
Our security approach is designed to safeguard client assets, support regulatory compliance, and provide assurance that all activities are conducted in a controlled, auditable, and secure manner.

Security measures include:

- Encryption of all engagement data at rest and in transit
- Secure credential handling and destruction
- Segregated and audited testing environments
- Privileged access management with least-privilege controls
- Personnel screening where appropriate
- Compliance with PTES, OSSTMM and OWASP standards
- Secure handling and deletion of client data

SAFEHARBOUR SECURITY

info@safeharboursecurity.com

www.safeharboursecurity.com

Catalyst Innovation Building, Bay Rd, Londonderry BT48 7TG

@ SafeHarbourSecurity