Penetration Testing

Service Description

V1.0 January 2025

Contents

1. Service Description 3
2. Service Operation 4
2.1. Internal infrastructure testing 4
2.2. External infrastructure testing 5
2.3. Web application testing 6
2.4. Mobile application testing 7
3. Service Bolt-Ons 9
3.1. Password analysis 9
3.2. Credential review 9
3.3. Phishing 10
3.4. Microsoft 365 security audit 11
3.5. API testing 12
4. Service Onboarding 14
5. Customer Obligations 15
6. Service Availability 16
7. Norm's Penetration Testing Credentials 17

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com

1. Service Description

Penetration Testing services from Norm provide security assessments of the Customer's computer networks, systems, applications, and people to identify and address security weaknesses.

Norm's highly trained security analysts will help the Customer to manage cyber security risks by identifying, safely exploiting, and helping to remediate weak points in the environment that could otherwise lead to data and assets being compromised, lost to malicious attackers, and possibly leading to other direct and indirect collateral damage/losses.

The Norm Penetration Testing services are comprised of the following key security assessment services:

- External Penetration Testing
- Internal Penetration Testing
- Web Application Penetration Testing
- Mobile Application Penetration Testing

Additionally, the following bolt-on components are available:

- Password analysis
- Credential review
- Phishing
- Microsoft 365 security audit
- API testing

2. Service Operation

2.1. Internal infrastructure testing

The Norm Internal Infrastructure Testing Service is designed to help the Customer understand the risk to the business should malicious insiders or attackers gain access to the Customer's systems. The Service involves the Norm Red team emulating the actions of these malicious actors and simulating real-world attack scenarios to uncover potential security gaps and provide actionable recommendations for mitigation against existing and potential threats.

Activities performed by the Norm red team may include, but are not limited to:

- **Threat modelling**: The Norm Red team will conduct a thorough analysis of the Customer's internal infrastructure, considering potential threats and attack vectors. This allows Norm to tailor the testing approach and prioritise high-risk areas to ensure the Customer derives maximum value from the engagement.
- **Exploitation and post-exploitation** : When a vulnerability is discovered, the Norm Red team will attempt to exploit them. This determines the extent to which a malicious actor could compromise the Customer's systems and gain unauthorised access. The Norm Red team will also assess the potential impact to the Customer of a successful attack.
- **Privilege escalation** : Commonly, malicious actors will attempt to exploit vulnerabilities or misconfigurations to elevate their privileges within the network, granting them greater access and control over systems and resources. Where an opportunity for privilege escalation is identified, the Norm Red team will attempt to leverage this and identify the opportunities for the Customer to enhance its access controls.
- **Data exfiltration**: The Norm Red team will assess the potential for data exfiltration by attempting to extract sensitive information (false, or real as defined in the scope of the test) from the Customer's internal system. This helps to identify potential data leakage risks and opportunities for improvement in the Customer's data protection measures.
- **Reporting and remediation** : Following the completion of the test, the Norm Red team will produce a comprehensive report detailing the team's findings including:
    - Discovered vulnerabilities
    - The risk those vulnerabilities pose to the Customer
    - Actionable recommended remediation measures

  The Norm Red team will present this report to the Customer's I.T. team to ensure that the risks are clearly communicated and understood, and that the Customer has the opportunity to ask any questions about the findings.
- **Re-test**: Upon request, the Norm Red team will perform a free re-test of any critical and high severity vulnerabilities discovered during the test to validate that the Customer's remediation efforts have been successful. The Norm Red team will then produce a report confirming whether the highlighted vulnerabilities have been fixed. Please note that the re-test must be performed within 90 days of receipt of the initial test report.

Optional Internal Infrastructure Testing bolt-ons:

- Password analysis (see 3.1)
- Credential review (see 3.2)

- Phishing (see 3.2)
- Microsoft 365 security audit (see 3.4)

2.2. External infrastructure testing

The Norm External Infrastructure Testing Service is designed to help the Customer understand the risk to the business should malicious actors attempt to gain access to the Customer's internet-facing systems, networks, or applications. The Service involves the Norm Red team emulating the actions of these malicious actors and simulating real-world attack scenarios to uncover potential security gaps and provide actionable recommendations for mitigation against existing and potential threats.

Activities performed by the Norm red team may include, but are not limited to:

- **Information gathering and reconnaissance**: Using passive techniques like OSINT (Open-Source Intelligence) the Norm Red team gathers information about the target organisation. This may include, domain names, IP addresses, email addresses, employee's names, and any other publicly available information. Norm will then enumerate DNS records to discover subdomains, mail servers, and other network-related information and perform a WHOIS lookup to obtain domain registration information to identify potential points of contact and infrastructure details.

- **Footprinting**: The Norm Red team will conduct port scans using tools such as Nmap to identify open ports, services, and potential entry points into the target network. Norm will also determine the services running on open ports to understand the attack surface and potential vulnerabilities, and extract banners from services to gather additional information about software versions and configurations.

- **Vulnerability analysis**: By performing vulnerability scans using tools such as Nessus, OpenVAS, or Qualys, the Norm Red team will identify known vulnerabilities in the target systems and applications. Using this information Norm will then research known exploits associated with the identified services and applications to prioritise potential attack vectors.

- **Exploitation and post-exploitation** : When a vulnerability is discovered, the Norm Red team will attempt to exploit them to ensure the accuracy and reliability of the findings. This determines the extent to which a malicious actor could compromise the Customer's systems and gain unauthorised access. The Norm Red team will also assess the potential impact to the Customer of a successful attack.

- **Reporting and remediation**: Following the completion of the test, the Norm Red team will produce a comprehensive report detailing the team's findings including:

    - Discovered vulnerabilities
    - The risk those vulnerabilities pose to the Customer
    - Actionable recommended remediation measures

  The Norm Red team will present this report to the Customer's IT team to ensure that the risks are clearly communicated and understood, and that the Customer can ask any questions about the findings. Norm will also support the Customer's remediation efforts by suggesting mitigation strategies.

- **Re-test**: Upon request, the Norm Red team will perform a free re-test of any critical and high severity vulnerabilities discovered during the test to validate that the Customer's remediation efforts have been successful. The Norm Red team will then produce a report confirming whether the highlighted vulnerabilities have been fixed. Please note that the re-test must be performed within 90 days of receipt of the initial test report.

Optional External Infrastructure Testing bolt-ons:

- Phishing (See 3.3)

2.3. Web application testing

The Norm Web Application Testing Service is intended to help the Customer understand the security of its applications and to identify vulnerabilities that might result in unauthorised access or data exposure. The Norm Red team will assess the Customer's web applications against the OWASP[1] Top 10, a list of the most critical web application security risks.

During a Web Application test the Norm Red team will evaluate the Customer's applications against:

- **Injection attacks (e.g. SQL, NoSQL, OS)** : The Norm Red team will assess the Customer's web applications for injection vulnerabilities that can allow attackers to execute malicious code or gain unauthorised access to its database by testing for SQL, NoSQL, and OS injections.
- **Cross-Site Scripting (XSS)** : The Norm Red team will analyse the Customer's web applications for XSS vulnerabilities, which can enable attackers to inject malicious scripts into trusted websites and compromise user data or spread malware.
- **Broken authentication and session management** : The Norm Red team will evaluate the authentication and session management mechanisms in the Customer's web applications to identify weaknesses that could lead to unauthorised access or session hijacking.
- **XML External Entity (XXE) attacks** : The Norm Red team tests the Customer's web applications for XXE vulnerabilities that can be exploited to read arbitrary files, perform server-side request forgery (SSRF), or launch denial-of-service attacks. By detecting and remediating XXE vulnerabilities, this is intended to prevent potential data leaks and service disruptions.
- **Broken access control**: The Norm Red team assesses the control mechanisms in the Customer's web applications to ensure that only authorised users can access sensitive resources and perform privileges actions. By identifying and addressing broken access control vulnerabilities, this is intended to prevent unauthorised access and data breaches.
- **Security misconfigurations** : The Norm. Red team examines the Customer's web application configurations, including servers, frameworks, and databases, to identify security misconfigurations that could exposes sensitive information or weaken the application's defences. Norm will provide recommendations to harden configurations and reduce the attack surface.
- **Cross-Site Request Forgery (CSRF)** : The Norm Red team analyses the Customer's web applications for CSRF vulnerabilities, which can lead to unauthorised actions being performed on behalf of authenticated users. By identifying and mitigating CSRT vulnerabilities, this is intended to prevent potential attackers from exploiting user trust and performing malicious activities.
- **Security headers and headers injection** : The Norm Red team assesses the presence and proper configuration of security headers in the Customer's web applications to enhance protection against various attacks, such as cross-site-scripting and clickjacking. Norm also

[1] The Open Worldwide Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software.

tests for headers injection vulnerabilities that could enable attackers to manipulate or bypass security measures.

- **Insecure deserialisation** : The Norm Red team examines the Customer's web applications for insecurity deserialisation vulnerabilities, which can lead to remote code execution, privilege escalation, or denial-of-service attacks.
- **Components with known vulnerabilities** : The Norm Red team scans the Customer's web applications for components (e.g., libraries, frameworks) with known vulnerabilities and provide recommendations for updating or replacing them with secure versions. This ensures that the Customer's understands if and where its applications contain any areas of weakness that potential attackers could exploit.

Following the testing phase, Norm will then complete the following activities:

- **Reporting and remediation** : Following the completion of the test, the Norm Red team will produce a report detailing the team's findings including:
    - Discovered vulnerabilities.
    - The risk those vulnerabilities pose to the Customer.
    - Actionable recommended remediation measures
- The Norm Red team will present this report to the Customer's IT team to ensure that the risks are clearly communicated and understood, and that the Customer can ask any questions about the findings. Norm will also support the Customer's remediation efforts by suggesting mitigation strategies.
- **Re-test**: Upon request, the Norm Red team will perform a free re-test of any critical and high severity vulnerabilities discovered during the test to validate that the Customer's remediation efforts have been successful. The Norm Red team will then produce a report confirming whether the highlighted vulnerabilities have been fixed. Please note that the re-test must be performed within 90 days of receipt of the initial test report.

Optional Web Application Testing bolt-Ons:

- API testing (See 3.5)

2.4. Mobile application testing

The Norm Mobile Application Testing Service is intended to help the Customer understand the security of its existing, or in development, mobile applications. With the proliferation of mobile devices and the increasing reliance on mobile applications for performing business functions, securing these applications to protect the business, and the end user, is paramount.

The Norm Red team will conduct a thorough assessment of the Customer's mobile applications across various platforms including iOS, Android, and hybrid applications. Norm will analyse the application's code, network communication, backend integrations, and overall architecture to identify potential security loopholes and vulnerabilities.

Activities performed by the Norm red team may include, but are not limited to:

- **Dynamic analysis**: The Norm Red team will perform dynamic analysis to assess the application's behaviour in real-time. Through dynamic testing, Norm can potentially identify runtime vulnerabilities, data leakage risks, and unauthorised access points that may compromise the security of the application and its users.

- **Static code analysis**: Utilising advanced static code analysis tools and techniques, Norm examines the application's source code for potential security weaknesses such as insecure coding practices, hardcoded credentials, and vulnerabilities that may lead to data breaches or unauthorised access.
- **Network security assessment** : The Norm Red team will assess the communication channels between the mobile application and backend servers to identify potential security risks such as data interception, man-in-the-middle attacks, and inadequate encryption protocols. The network security assessment confirms whether data transmitted between the application and servers remains secure and encrypted.
- **Backend security evaluation** : In addition to assessing the mobile application itself, Norm also evaluates the security posture of backend servers, APIs, and databases that the application interacts with. This comprehensively evaluates the end-to-end security across the entire application ecosystem.
- **Reporting and remediation**: Following the completion of the test, the Norm Red team will produce a comprehensive report detailing the team's findings including:
    - Discovered vulnerabilities
    - The risk those vulnerabilities pose to the Customer
    - Actionable recommended remediation measures

  The Norm Red team will present this report to the Customer's IT team to ensure that the risks are clearly communicated and understood, and that the Customer can ask any questions about the findings. Norm will also support the Customer's remediation efforts by suggesting mitigation strategies.
- **Re-test**: Upon request, the Norm Red team will perform a free re-test of any critical and high severity vulnerabilities discovered during the test to validate that the Customer's remediation efforts have been successful. The Norm Red team will then produce a report confirming whether the highlighted vulnerabilities have been fixed. Please note that the re-test must be performed within 90 days of receipt of the initial test report.

3. Service Bolt-Ons

- Password analysis
- Credential review
- Phishing
- Microsoft 365 security audit
- API testing

3.1. Password analysis

Available as part of an internal test.

The Active Directory (AD) Password Analysis Service is a comprehensive solution designed to evaluate the strength, security, and adherence to best practice of user passwords within an organisation's Active Directory environment. This Service provides insights into password practices, identifies potential vulnerabilities, and assists in enhancing overall cyber security posture.

Activities performed by the Norm red team may include, but are not limited to:

- **Password strength assessment** : The Service thoroughly examines the strength of passwords across the Active Directory, analysing factors such as length, complexity, and patterns to determine their susceptibility to brute-force attacks and dictionary-based cracking.
- **Policy compliance evaluation** : It assesses password policies configured within Active Directory against industry standards and organisational requirements. This includes parameters like minimum length, complexity requirements, expiration intervals, and history constraints.
- **Risk identification** : The Service identifies high-risk passwords, including commonly used or easily guessable phrases, dictionary words, and sequential or repetitive patterns. It also detects passwords that have been compromised in data breaches and may be present in leaked credential databases.
- **User behaviour analysis** : Analysing password usage patterns and trends among users provides insights into potential security weaknesses and areas for improvement. It helps in identifying users who frequently reuse passwords across multiple accounts or who choose weak passwords.
- **Reporting and recommendations** : Detailed reports are generated highlighting findings, including areas of concern, non-compliant passwords, and recommended actions for improving password security. These reports are tailored to both technical and managerial audiences, facilitating informed decision-making and prioritisation of remediation efforts.

3.2. Credential review

Available as part of an internal test.

The Norm Credential Review Bolt-on Service is a type of security assessment conducted on a network, system, or application using authenticated access credentials. Unlike non-credentialed scans, which rely on external observation and network-based assessments, credentialed scans have privileged access to the target system, allowing the scanner to probe deeper into the system's configuration, settings, and installed software.

Activities performed by the Norm red team may include, but are not limited to:

- **Authentication**: Credentialed vulnerability scans require valid login credentials, such as usernames and passwords, to access the target system or application. These credentials provide the Norm scanner with elevated privileges to gather detailed information about the systems configuration, installed software, and user settings.
- **Detailed assessment** : With authenticated access, the Norm vulnerability scanner can perform a more comprehensive assessment of the target systems security posture. It can analyse the systems registry settings, file permissions, installed patches, running services, and other critical components that may not be accessible during non-credentialed scans.
- **Accurate identification of vulnerabilities** : Credentialed scans enable the Norm vulnerability scanner to accurately identify vulnerabilities present on the target system by comparing its configuration against a comprehensive database of known vulnerabilities and security misconfigurations. This allows organisations to prioritise and remediate vulnerabilities based on their severity and potential impact.
- **Reduced false positives** : Since credentialed scans have access to detailed system information, they can reduce the number of false positives generated during the assessment. By correlating scan results with the actual system configuration, the scanner can distinguish between legitimate configurations and potential security issues more accurately.
- **Compliance requirements** : Credentialed vulnerability scans are often required to meet regulatory compliance standards and industry best practices. Many compliance frameworks, such as PCI DSS mandate the use of authenticated scans to assess the security posture of systems and applications accurately.
- **Enhanced remediation recommendations** : Authenticated vulnerability scans can provide more actionable remediation recommendations tailored to the specific configuration and software environment of the Customer's systems. This enables the Customer to address vulnerabilities more effectively and implement security controls that align with its operational requirements.
- **Operational impact**: Credentialed scans may have a higher operational impact compared to non-credentialed scans, as they require valid credentials and access to the target system. Norm will plan carefully with the Customer to schedule credentialed scans to minimise disruption to minimise disruption to critical business operations and ensure proper authorisation and oversight.
- **Reporting and remediation**: Following the completion of the test, the Norm Red team will produce a comprehensive report detailing the team's findings including:
    - Discovered vulnerabilities
    - The risk those vulnerabilities pose to the Customer
    - Actionable recommended remediation measures

  The Norm Red team will present this report to the Customer's IT team to ensure that the risks are clearly communicated and understood, and that the Customer can ask any questions about the findings. Norm will also support the Customer's remediation efforts by suggesting mitigation strategies.

3.3. Phishing

Available as part of an internal or external test.

The Norm Phishing Bolt-on Service offers a proactive approach to assess and enhance the security awareness and resilience of the Customer against phishing attacks. Phishing remains one of the most prevalent and effective methods used by cyber criminals to gain unauthorised access to sensitive information, compromise systems, and infiltrate networks. Norm will simulate real-world phishing scenarios to evaluate the Customer's susceptibility to such attacks and provides actionable insights to strengthen its security posture.

- **Customer phishing campaigns** : Norm will design and execute customised phishing campaigns tailored to the specific needs and requirements of the Customer. The Red team creates realistic phishing emails, text messages, and social engineering scenarios that mimic the tactics employed by real attackers, ensuring a highly authentic simulation.
- **Targeted audience engagement** : Norm will target different user groups within the organisation, including employees, executives, and contractors, to assess the effectiveness of security awareness training programs and identify areas for improvement. By targeting diverse user segments, Norm can provide a comprehensive assessment of the Customer's overall susceptibility to phishing attacks.
- **Multi-vector phishing simulations** : Norm will employ various phishing vectors and techniques, including email, SMS, voice calls, and social media, to simulate a wide range of phishing scenarios. This multi-vector approach measures the Customer's preparedness to defend against different types of phishing attacks and social engineering tactics commonly used by cyber criminals.
- **Real-time monitoring and analysis** : Throughout the duration of the phishing campaign, the Red team monitors user interactions, click rates, and response patterns in real-time. Norm will analyse the data collected from phishing simulations to identify trends, patterns, and areas of vulnerability within the Customer's security infrastructure.
- **Detailed reporting and recommendations** : Norm will deliver detailed reports outlining the results of the phishing engagement, including metrics such as click rates, response rates, and susceptibility levels across different user groups. The reports also include actionable recommendations and remediation strategies to address identified vulnerabilities and strengthen the organisation's resilience against phishing attacks.

3.4. Microsoft 365 security audit

Available as part of an internal test.

The Norm Microsoft 365 (M365) Security Audit Bolt-on Service evaluates the customer's M365 environment's security. The Norm Red team simulates real attacks to find vulnerabilities, using tools like Nmap, PowerShell, and specialised M365 tools. Norm will identify weak spots in authentication, access controls, and data protection, resulting in a detailed report with actionable suggestions.

Activities performed by the Norm red team may include, but are not limited to:

- **Assessment**: The Norm Red team will assess the Customer's M365 setup, including Exchange Online, SharePoint, Teams, and Entra ID.
- **Simulated attacks**: By mimicking real threats used by attackers, the Norm Red team will uncover weaknesses in the Customer's configurations.
- **Tool-based analysis**: Norm will use various tools like Nmap, PowerShell, and specialised M365 tools for testing.

- **Reporting and remediation**: Following the completion of the test, the Norm Red team will produce a comprehensive report detailing the team's findings including:

    - Discovered vulnerabilities
    - The risk those vulnerabilities pose to the Customer
    - Actionable recommended remediation measures

    The Norm Red team will present this report to the Customer's IT team to ensure that the risks are clearly communicated and understood, and that the Customer can ask any questions about the findings. Norm will also support the Customer's remediation efforts by suggesting mitigation strategies.

3.5. API testing

Available as part of a web application test.

The Norm API Testing Bolt-on Service is designed to identify, and support the remediation of, security vulnerabilities within the Customer's application's API (Application Programming Interface) infrastructure. APIs play a crucial role in modern software development, facilitating seamless communication and data exchange between different components. However, their exposure also introduces potential security risks. The Norm Red team employs advanced methodologies to assess the security posture of the Customer's APIs, to measure its resilience against known threats.

- **Thorough API assessment**: The Norm Red team will conduct a comprehensive assessment of the Customer's API endpoints, scrutinising each element for potential vulnerabilities. This includes API endpoints, authentication mechanisms, data validation, and error handling.
- **Security standards compliance**: Norm will evaluate the Customer's APIs against industry standards and best practices, such as OWASP API Security Top 10, to ensure compliance and adherence to security guidelines.
- **Authentication and authorisation testing**: Rigorous testing of authentication and authorisation mechanisms is performed to identify weaknesses that could lead to unauthorised access or data exposure.
- **Data validation and input testing**: Norm scrutinises input parameters and data validation processes to prevent common security issues like SQL injection, cross-site scripting (XSS), and other injection attacks.
- **Encryption and transport layer security**: Assessment of the encryption methods and the implementation of secure communication channels to guarantee data confidentiality and integrity during transmission.
- **Rate limiting and throttling analysis**: Examination of rate limiting and throttling controls to prevent abuse and mitigate the risk of denial-of-service (DoS) attacks.
- **API documentation review**: A review of API documentation to ensure it does not inadvertently expose sensitive information and accurately reflects security considerations for developers.
- **Penetration testing tools utilisation**: Norm leverages industry-leading penetration testing tools and methodologies to simulate real-world attacks and discover vulnerabilities that may not be apparent through standard testing.

- **Remediation guidance and reporting** : Detailed reports are provided, outlining discovered vulnerabilities, their potential impact, and actionable recommendations for remediation.

Before this bolt-on Service can be delivered, the Customer must provide API documentation and output examples.

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com

4. Service Onboarding

Once an order is received, a member of the Norm Customer Experience team will get in touch and take responsibility for managing the delivery process. They will provide the Customer with an administrative account for the Smartbloc portal and introduce a nominated Norm Red Team Consultant who will be responsible for delivering the Service and providing the final report.

They will:

- Arrange a technical scoping call between a member of the Red team and the Customer's IT team (or managed service provider (MSP)) to identify the systems, applications, and network segments to be tested. The scope will be clearly defined for the engagement to ensure that it aligns with the Customer's specific objectives and requirements.
- Document the scope of the Penetration Test assessment Service and ask the Customer to agree and sign off. This will include defining any technical infrastructure to be deployed for the testing.
- Agree a testing window in which the test will be conducted. The testing team will be on call throughout the testing and available for any questions that may arise.

The Customer will ensure that any required infrastructure to support the testing is deployed and Norm is provided with access to the environment no later than five days prior to the agreed commencement date of the test. Where these conditions are not met or

Once the test has been completed, Norm will provide a report detailing the findings of the above tests, as well as remediations steps and/or best practice recommendations to address any issues found.

Reports will be provided via the Smartbloc portal.

Norm will offer the Customer the opportunity to review the results of the test with the testing team to help the Customer understand exactly what vulnerabilities were discovered, how they could be taken advantage of, and how to remediate these vulnerabilities.

If requested, Norm will provide a free re-test on all 'Critical' and 'High' category vulnerabilities to ensure that they have been remediated appropriately. The Service only includes re-tests that occur within 90 days of the date the report is provided.

5. Customer Obligations

Once the Order is accepted, the Customer shall,

- provide an Authorised Representative who shall be the Customers Administrator and Authorised Signatory for the acceptance of the Services and responsible for creating and managing access for other Customer End Users who need access to the Service or Smartbloc portal
- agree a timely schedule with Norm's Red Team Consultant to agree the Scope of the Penetration Test and ensure the accuracy of the information provided, for Norm to be able to deliver the Services
- provide any documentation, schematics, access credentials, infrastructure or other information as so required to perform the test, within ten (10) Working days after it has been requested by Norm's Red Team Consultant, and, in any case, at least five (5) Working days prior to the date that the Penetration Test is scheduled to commence
- ensure that all necessary notices have been provided, and all required consents and/or approvals have been obtained, in order to allow Norm to process the Customer's Data in connection with the Services
- be wholly responsible for delays in the delivery of the Service, where it has not provided the information requested to perform the Service or returned the relevant Authorisation documentation to allow Norm to commence the Service. Where the Customer delays the delivery of the Service, for any reason, Norm reserves the right to cancel the Service, and the Customer will remain liable for all charges payable in relation to the Service
- ensure that its employees and other independent contractors co- operate fully with Norm in relation to the provision of the Services
- use the Services only in accordance with this Agreement, and all applicable laws and regulations

The Customer shall not,

- make the Services available to anyone other than the Authorised Representatives
- sell, resell, rent, lease, lend, loan, distribute, sublicense or otherwise assign or transfer the Services or any rights thereto in whole or in part
- use the Services to store or transmit infringing, libelous, or otherwise unlawful or taurus material, or to store or transmit material in violation of third-party rights (including privacy rights)
- use the Services to store or transmit Malicious Code
- interfere with or disrupt the integrity or performance of the Services or third-party data contained therein
- attempt to gain unauthorised access to the Services or related systems and/or networks, or
- use the Services in any manner that would cause NormCyber to be in violation of any laws, rulings or regulations

6. Service Availability

The Norm Red Team Consultants and Customer Experience team are available during UK business hours, Monday to Friday 09:00 to 17:30, excluding public holidays. Where the Customer wishes to conduct a test outside of these hours, this is possible, but maybe subject to additional Charges.

7. Norm's Penetration Testing Credentials

Norm's penetration testing services are CREST accredited which provides independent assurance that Norm Red team penetration testers have passed rigorous professional examinations to demonstrate their knowledge, skills and competencies. CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market. Norm's membership demonstrates its commitment to ensuring the highest quality standards are maintained, by utilising highly skilled, knowledgeable and competent individuals.

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com