Penetration Testing Policy

Section 1 - Overview

(1) This Policy sets out our commitment to conducting penetration tests in a controlled, responsible and proportionate manner to identify and validate vulnerabilities while protecting our information, information assets, products and services.

(2) Penetration Tests are is undertaken to strengthen the security of our products, services and information assets by identifying and validating vulnerabilities and supporting their timely remediation. It is intended to demonstrate the existence and potential impact of vulnerabilities using the minimum level of access, interaction and information necessary to achieve the objectives of each engagement.

(3) We recognise that penetration tests are an important component of our broader information security framework and will be undertaken in a manner that balances effective security assurance with the protection of our information, information assets, products, services and the interests of our clients.

Section 2 - Scope

(4) This Policy applies to all penetration tests undertaken by or on our behalf in relation to our products, services and information assets.

(5) This Policy applies whether penetration tests are undertaken by our personnel or by third parties acting on our behalf.

Section 3 - Policy

(6) We will ensure that penetration tests:

a. are undertaken at intervals appropriate to the level of risk presented by our products, services and information assets;
b. are undertaken following significant changes that may materially affect the security of our products, services or information assets;
c. are authorised before testing commences;
d. are conducted only within an approved scope;
e. are planned and undertaken in a manner that minimises the risk of disruption to our operations and the operations of our clients;
f. are conducted using techniques that are proportionate to the objectives of the engagement;
g. are undertaken in accordance with applicable legislation, contractual obligations and our corporate governance framework;
h. demonstrate the existence and potential impact of vulnerabilities using the minimum level of access, interaction and information necessary to achieve the objectives of the engagement; and
i. are appropriately documented and reported.

(7) Where penetration testing results in access to information or information assets, we require that:

a. only the minimum access reasonably necessary to validate the vulnerability is obtained;
b. examination of information ceases as soon as sufficient evidence has been obtained to validate the vulnerability;
c. information is not intentionally browsed, searched, analysed or otherwise examined beyond that reasonably necessary to validate the vulnerability;
d. information is not copied, extracted, retained or disclosed except where necessary to document the finding;
e. all information included in evidence or reports is limited to the minimum necessary to support the finding;
f. where evidence or reports contain sensitive information or confidential information, that information is excluded or redacted wherever reasonably practicable;
g. information obtained during testing is appropriately protected while retained; and
h. information obtained during testing is securely disposed of when it is no longer required for the purposes of the engagement.

(8) Unless expressly authorised in writing, penetration tests must not:

a. intentionally disrupt or degrade production services;
b. intentionally alter, delete or corrupt information;
c. establish persistent or ongoing access to any system;
d. exceed the approved scope of the engagement; or
e. disclose information obtained during testing to any unauthorised person.

Section 4 - Procedures

(9) Procedures are agreed for each authorised penetration test, aligned with this Policy.

Section 5 - Guidelines

(10) Nil.

Section 6 - Definitions

(11) Definitions applicable to this Policy are contained in the Corporate Glossary.

Status and Details

Status	Current
Effective Date	26th June 2026
Review Date	26th December 2028
Approval Authority	Director
Approval Date	26th June 2026
Expiry Date	Not Applicable
Responsible Manager	Joanne Auld Director
Author	Joanne Auld Director
Enquiries Contact	Joanne Auld Director

Glossary Terms and Definitions

"Confidential Information" - Means information that is not publicly available and which, if disclosed, accessed, altered or destroyed without authorisation, could reasonably be expected to prejudice the interests of the Organisation, its clients, business partners or other stakeholders. Confidential Information includes, but is not limited to, commercial information, contractual information, intellectual property, security information, technical information, financial information, and personal information that is not otherwise publicly available.

"Information Asset" - Means any information, regardless of form or medium, together with the systems, applications, infrastructure, services or components used to create, collect, process, store, transmit, protect or dispose of that information, where the loss, compromise or unavailability of the asset could affect the Organisation or its stakeholders.

"Penetration Test" - Means an authorised security assessment conducted using techniques intended to identify and validate vulnerabilities by attempting to compromise systems, applications, infrastructure, networks or other Information Assets under controlled conditions.

"Sensitive Information" - Means information that requires protection because unauthorised access, use, disclosure, modification or destruction could reasonably be expected to result in harm to an individual, the Organisation, a client, business partner or other stakeholder, whether or not the information is classified as Confidential Information. Sensitive Information includes personal information, security credentials, authentication information, financial information, commercially valuable information and other information identified by the Organisation as requiring additional protection.

"Vulnerability" - Means a weakness, deficiency or flaw in a system, application, process, configuration, control or operational practice that may be exploited to adversely affect the confidentiality, integrity or availability of information or other information assets, the security or operation of the Organisation, or the rights, interests or wellbeing of individuals or other stakeholders.

"Information" - Means knowledge or data, regardless of form or medium, including electronic, physical, verbal or visual information.

"Information Security" - Means the preservation of the confidentiality, integrity and availability of Information Assets through the implementation of appropriate administrative, physical and technical controls.

"Product" - Means any software, platform, module, component, application or other offering developed, licensed, supplied or maintained by the Organisation.

"Service" - Means any activity performed by or on behalf of the Organisation for the benefit of a client or stakeholder, including support, implementation, consulting, hosting, maintenance or managed services.