



Penetration Testing Service Schedule

This Service Schedule forms part of the Agreement between You and Superloop and is applicable to Services entered into between You and Superloop.

The Penetration Testing Services are a set of cyber security tools that Superloop provides to assist in making Your network and environment more secure. Superloop is not responsible for the security of Your business or any loss or damage to Your business. The Penetration Testing Services do not replace a comprehensive information security plan.

1. Service Description

1.1 General

The Service is comprised of the following items ("Penetration Testing Services"):

- (a) Access to Penetration Testing Reports for Your test and not the Superloop platform that runs them;
- (b) Configuration of the Penetration Testing platform;
- (c) All applicable software licences;
- (d) The provisioning of any internal devices in accordance with Your Security Policy;
- (e) A one-time follow-up post-run test, to be conducted within four weeks that is included with our comprehensive one-time Penetration Testing Services; and
- (f) A monthly report available to download for all SuperScreen Penetration Tests.

1.2 Penetration Testing Platform

The platform provides you with the ability to:

- (a) Monitor Your environment and network;
- (b) Generate Penetration Test reports; and
- (c) Access will be granted to the reports and not the platform.

2. Provision of Services

2.1 Provisioning

- (a) Superloop will provision the Penetration Testing Platform and any internal devices to perform the Penetration Test as per Your Service Order.
- (b) The Penetration Testing Platform is used and deployed as a black-box test, no details of the platform will be presented to You.
- (c) Superloop will provide You with detailed information of any required internal firewall changes needed to facilitate an internal test.
- (d) The SuperScreen Penetration Test is fully automated end-to-end service that tests against Superloop links and IP addresses and will deliver all reports into your customer portal.

2.2 Use of the Service

You:

- (a) will grant us permission to perform the Penetration Testing Services in accordance with the Agreement and any applicable Statement of Work / Service Order.
- (b) will be required to secure all necessary authorisations from Third Parties to allow us to carry out the Penetration Testing Services (if required) and provide proof of these authorisations when requested.
- (c) will guarantee that the execution of the Penetration Testing Services is lawful in Your location and where Your systems are situated. You acknowledge that we will deliberately attempt to bypass security controls to access Your systems and data, and that such actions would otherwise be considered criminal activity on our part.
- (d) acknowledge that Penetration Testing Services carry inherent risks. While we will take reasonable precautions to perform the Services, to the fullest extent permitted by law, we are not responsible for any losses or downtime that may result from these Services.
- (e) guarantee that You will assess the impact and associated risks of implementing any recommendations We provide in our reports. You are in the best position to determine the suitability of security procedures and updates for Your environment.
- (f) acknowledge that We depend on the timeliness and accuracy of the information You supply.
- (g) must promptly confirm to any external body, including law enforcement agencies, that We were acting with proper authorisation should You report any actions we perform as part of the Penetration Testing Services.
- (h) must indemnify Us against any claims, costs, losses, or liabilities that may arise due to Your breach of any obligation or warranty under this clause. This indemnity is not subject to the limitations and exclusions of liability outlined in the Agreement (if any).

2.3 Termination

At the expiry of the Service Term or upon a valid termination of the Service by either party, You will promptly return or delete any Confidential Information that You have received from Superloop during the Service Term of the Agreement.

For any Penetration Testing Service that is tied to a minimum term contract, a Cancellation Charge will be applicable for any early termination of the Services.

3. Our Personnel and Assistance

3.1 Our Personnel

- (a) When Our Personnel perform the Penetration Testing Services at Your Site, You will ensure that Your Site complies with all applicable health, safety, environmental, and community laws and regulations.
- (b) You will obtain any necessary consents and cover any Site access and induction fees required to enable Our Personnel to access Your Site and perform the Penetration Testing Services.
- (c) You must not, and must ensure that Your employees, contractors, or agents do not, attempt to gain unauthorised access to accounts, computer systems, or networks in connection with the Penetration Testing Services through hacking, password mining, or any other means. You must not obtain or attempt to obtain any materials or information through any means not intentionally made available through the supply of the Penetration Testing Services.
- (d) You must not, and must ensure that Your related bodies corporate do not, during the Restraint Period, seek to employ or engage the services of any of Our Personnel involved in providing the Penetration Testing Services to You. This does not apply to a person who responds to a genuine published advertisement. You acknowledge that the Restraint Period in this clause is reasonable in its extent and goes no further than is necessary to protect Our interest in maintaining Our Personnel.

3.2 Assistance

You must:

- (a) provide Us with all information or assistance that We reasonably request or that is otherwise necessary to supply the Penetration Testing Services, including by:
 - (i) make Your staff available to answer questions; and
 - (ii) ensure Your third-party suppliers cooperate with Us and provide Us with any information and assistance We reasonably require;
- (b) provide Us with test user accounts if required;
- (c) notify Us in advance (no less than 48 hours) of any planned downtime for the environment used in the Penetration Testing Services;
- (d) ensure that You do not block our Penetration Testing Services' traffic to the environment;
- (e) ensure that all information provided to Us is accurate and complete;
- (f) grant us access to Your network, systems, and Site with reasonable notice;

- (g) If Penetration Testing Services are to be conducted in a test environment (as detailed in the Statement of Work / Service Order), ensure the test environment:
 - (i) is available to Us within the agreed timeframes;
 - (ii) mirrors Your systems' live production environment;
 - (iii) is dedicated to Us for the Penetration Testing Services, and is otherwise suitable for the Penetration Testing Services; and
 - (iv) is segregated from any live production environment or data in a way that avoids or minimises the potential for detrimental impact to such live production environments or data.
- (h) After the Penetration Testing Services have been completed, restore or remove from Your systems and data, files and user accounts created in connection with the Penetration Testing Services.
- (i) You must appoint at least one appropriately skilled and qualified member of Your staff to liaise with Us on all matters relating to the Penetration Testing Services.

4. Risks and Adverse Impacts

4.1 Access Risk

- (a) You understand the Penetration Testing Services will involve access to data and systems accessible via Your systems and there is a risk that the Penetration Testing Services may result in:
 - (i) damage, loss, modification or impairment of such data and systems (including in respect of reliability, security, performance and operation);
 - (ii) reduction in the availability of network services and functionality; and
 - (iii) impairment of electronic communications.

4.2 Penetration Testing Limitations

You understand that the Penetration Testing Services:

- (a) may not identify all vulnerabilities within Your systems;
- (b) are limited to an assessment of the current state of Your environment; and
- (c) will not produce particular results or outcomes (including achieving any external accreditation or industry standard).

4.3 Assessment

You must make your own assessment of the information and any recommendations provided by Us and must satisfy Yourself as to its appropriateness for Your specific requirements, prior to implementing any recommendation We provide.

4.4 Industry Practice

You must use Good Industry Practice procedures and measures to avoid or minimise the impact of the risks identified in this clause, including by ensuring that:

- (a) the data and systems accessible via Your systems are backed up regularly; and
- (b) the back-ups are promptly restored, if required.

4.5 Material Adverse Impact

If You reasonably believe that the Penetration Testing Services are materially adversely impacting any person, system or data, You:

- (a) must notify Us as soon as possible; and
- (b) may direct us to suspend the Penetration Testing Services if reasonably required to minimise the material adverse impact.

4.6 Suspending the Service

If You direct Us to suspend the Penetration Testing Services in accordance with clause 4.5, We will:

- (a) suspend the Penetration Testing Services as soon as possible; and
- (b) meet with You within 24 hours (or such other agreed period) to agree the timeframe to resume Penetration Testing Services and any changes reasonably required to minimise the likelihood the material adverse impact will recur.

5. Privacy

5.1 Use of Your Personnel Information

You agree and consent that:

- (a) We may use and disclose Personal Information that is made available to Us as is reasonably required in order to provide the Penetration Testing Services to You including disclosing Personal Information to Third Parties including Our subcontractors and suppliers who provide Services to Us; and
- (b) We may use or disclose Personal Information in accordance with the Superloop Privacy Statement (available at <https://files.superloop.com/terms/SL-Residential-privacy-policy.pdf>), this section of Our Penetration Testing Service Schedule and in accordance with our Agreement with You.

5.2 Using and Collecting Personal Information

You agree and consent that:

- (a) You have taken all steps necessary in accordance with Privacy Laws to permit Us and any Third Parties who provide services to Us to collect Personal Information and to use,

disclose, store and transfer such Personal Information as contemplated under this clause; and

- (b) You have notified or made the relevant individual aware of the matters, required in relation to notification of the collection of Personal Information under Privacy Laws, in respect of the use and disclosure of that individual's Personal Information as contemplated under this clause.

5.3 Indemnifying Superloop

- (a) You indemnify Us against any claim, cost, loss or liability which may arise in connection with Your breach of the warranty in clause 5 above.

6. Your Obligations

6.1 Provisioning

In order for Superloop to provision the Service, You must:

- (a) provide accurate and complete information to Superloop as required for the deployment of the Service. You may be liable for any costs incurred by Superloop due to any incorrect, false or misleading information You provide; and
- (b) perform any changes to firewalls or infrastructure to facilitate the Internal Penetration test, as required.

7. Defined terms

All other capitalised terms in this Penetration Testing Service Schedule have the following meaning, unless the context otherwise requires:

Agreement means the agreement between Superloop and You (incorporating the General Terms, this Service Schedule, and any applicable Service Order) in relation to the supply of Services by Superloop to You, which is available at <https://superloop.com/legal/terms/>.

Cancellation Charge means an amount equal to the monthly recurring charge payable for the terminated Service multiplied by the number of months, or part thereof, between the date of termination and the end of the Service Term.

Good Industry Practice means the practice of a reasonable and prudent operator in the same business as the party required to comply with good industry practice.

Penetration Testing Platform refers to the cloud-based platform utilised for conducting penetration testing activities.

Personnel means the employees, contractors, agents, and any other individuals or entities engaged by the service provider to perform the agreed-upon services.

Restraint Period means the non-solicitation of our Personnel for a period of at least 12 months following the completion of any ongoing projects

Security Policy means the controls, rules, and/or configuration as agreed by the parties.

Service means the Penetration Testing Services as described in clause 1 and specified in a Service Order.

Site means each of Your physical premises, including Facilities, located at the site addresses specified in the Service Order.

SuperScreen Penetration Test means the scaled down Penetration Test that focuses only on the IP address of the link we provide and which this service has been added to, which differs from the full External or Internal Penetration Test which has more features and flexibility.

Third Party means a person other than Superloop or its Affiliates (and their respective officers, employees, agents and subcontractors), including Acurus Pty Ltd which may perform some aspects of the Services.