# AGREEMENT APPLICABLE TO PENETRATION TESTS AUTHORISED BY PENNYLANE SAS

Version applicable as from 16.09.2026 / v2026.09

**Penetration test initiated by a third-party is the exception: please consider our standard process first**

Pennylane is subject to strict security standards and has implemented state-of-the-art security measures, independently tested at least once a year; because the Solution is used by thousands of clients and partners, only a very limited number of client-run tests can be authorised, and only within the precise framework set out below.

Pennylane already commissions independent penetration tests at least once a year and is ISO 27001 certified. Before requesting a Test, any client is encouraged to ask for the available resources available, either online at any time (Security whitepaper, Incident Response Plan, ISO 27001 certificate) or on demand after signature of an NDA (existing PenTest summary report).

**Tolerance for basic internal phishing awareness campaigns**.

By way of exception to section 3, a client of Pennylane may run ordinary internal phishing awareness campaigns, consisting of plain emails sent to its own people, without seeking Pennylane's authorisation, provided that all three of the following conditions are satisfied at all times:

a. **Recipients**. No one outside the client's own staff is targeted, and in particular no Pennylane employee, no customer or supplier of the client, and no user belonging to another organisation. Staff must not be prompted to contact Pennylane support, report fraud to Pennylane or perform a real operation in the Solution.

b. **No use of Pennylane's identity or interfaces (except the limited and fair use of name and logo)**. No domain name containing or imitating "Pennylane" is registered or used (including typosquatted, look-alike or misleading domains and subdomains), no @pennylane.com sender is spoofed, and the Solution's login portal, interface, screens are never reproduced, cloned or imitated. Any debrief page must state clearly that this is an internal exercise and that Pennylane is not its author.

c. **No credential collection**. No authentication data is ever requested, collected, stored, transmitted or displayed — no passwords, one-time codes, MFA tokens, session cookies, API keys or security question answers — whether relating to the Solution or to any other service. A landing page may record that a link was clicked; it must capture nothing else.

Any other campaign must follow the provisions of this Agreement (in particular section 6).

## 1. PURPOSE AND SCOPE

This agreement (the "**Agreement**") sets out the mandatory conditions applicable to any third-party tester (the "**Tester**") who Pennylane has expressly authorised to run a security test on the Solution, and whose Test is not commissioned by Pennylane.

It covers every form of security testing, whatever its name, method or scope: penetration tests (black, grey or white box) on web, mobile and API interfaces; vulnerability scans and automated testing; phishing simulations run to raise awareness among the Tester's staff and reproducing any part of Pennylane's Solution, brand, domains or communications; and any other offensive testing, red teaming or social engineering (each, a "**Test**").

If the Tester is a client or partner of Pennylane, in any country where Pennylane operates (and regardless of Pennylane's contracting entity), the Agreement supplements the applicable standard terms or specific contract for the use of the Solution. Standard terms already prohibit any security test carried out by a client or partner without Pennylane's prior written authorization. In case of conflict, such applicable contract prevail.

The Tester is deemed to accept the Agreement when submitting an authorisation request.

## 2. DEFINITIONS

**Authorisation** = Pennylane's written and express approval following a valid request as per the process below

**Scope** = the exhaustive list of assets, environments, accounts, URLs, domains and scenarios approved

**Test Window** = the approved dates and hours

**Third-Party Data** = any data not belonging to the Tester (other clients, partners, Pennylane, its staff or subcontractors)

**Testing Provider** = any third party engaged by the Tester to run all or part of the Test

**Pennylane** = a simplified joint-stock company, registered in France with the Paris trade and companies Register under number 880 265 921, whose registered office is at 2-4 rue Jules Lefebvre, 75009 Paris, France,

**Solution =** refers to all computer programmes published by Pennylane in 'SaaS' mode, the features of which are described on its website and in its documentation, including updates, accessible via an internet connection, using a web interface or a mobile application. The Solution also includes all intellectual works, in particular all literary, artistic, graphic and audiovisual works, database structures and data created by Pennylane or in respect of which Pennylane holds the right to exploit.

## 3. GOLDEN RULE: NOTHING STARTS WITHOUT WRITTEN APPROVAL

### 3.1. Prior authorisation

No Test may be prepared in an active way (intrusive reconnaissance, scanning, registering a look-alike domain), started or run **without Pennylane's prior written Authorisation**. Silence never means approval, and a past authorisation never covers a new Test.

### 3.2. Single channel

Requests must be sent **exclusively** to security@pennylane.com. Requests made through any other channel (support chat, CSM/KAM, Slack Connect, an employee's personal email, Service Desk ticket) are not admissible and can never constitute approval — even if the person contacted replies positively.

### 3.3. Lead time

Requests must be submitted at least **15 business days** before the intended start date. Pennylane will aim to reply within **10 business days** of receiving a complete request (this lead time is not binding, and an absence of answer means that the request is refused).

### 3.4. Mandatory content

A request is incomplete — and therefore rejected — unless it includes:

- **The requester**: legal entity, company number, insurance certificate, authorised signatory, named individuals acting on its behalf, and an operational contact reachable at all times during the Test.
- **A detailed description of the Test**: objectives, methodology and type (black / grey box), framework used (OWASP, PTES…), tools, attack scenarios, volume and intensity (requests per second, number of accounts).
- **The requested Scope**: exhaustive list of URLs, subdomains, APIs, mobile apps, accounts and environments — and an explicit list of exclusions.
- **Dates and hours**, including time zone.
- **Expected impact** on availability, integrity, performance, invoicing, banking flows and end users; mitigation measures; emergency stop (kill switch) procedure and how fast it can be triggered.
- **Data collected**: what data may be accessed, collected, extracted or generated, stating clearly whether or not it includes personal data, together with purpose, legal basis, retention, hosting location, security measures, deletion process and any DPIA.
- **The Testing Provider, if any**: legal entity, country, certifications (e.g. PASSI, CREST, OSCP), named individuals acting on its behalf, source IP ranges and identifying user-agent, signed NDA and insurance certificates.
- **For phishing campaigns**: the additional items in section 6.

### 3.5. Pennylane's decision

A Test is not a standard process at Pennylane and an Authorisation shall be considered as an exception.

Pennylane grants or refuses Authorisation **at its sole discretion and without having to give reasons** — for instance for security, service continuity, regulatory or scheduling reasons (freeze periods: closings, tax and filing deadlines, migrations, ongoing incidents).

### 3.6. Conditions and limits

Authorisation may be subject to conditions (reduced Scope, mandatory use of a dedicated environment, request-rate cap, joint supervision, dedicated test accounts, specific HTTP header). It is **strictly limited** to the Scope, Test Window, named individuals and methods it lists; any change, however minor, requires a new written approval before it is implemented.

### 3.7. Revocation

Pennylane may suspend, restrict or revoke the Authorisation **at any time, without notice, without compensation and without justification**. The Tester must then stop all testing activity immediately, and in any event within **1 hour**.

### 3.8. Frequency and costs

Unless agreed otherwise, the Tester must not submit frequent or successive requests for Test. Pennylane may charge for its standard support work (preparation, supervision, dedicated environment) at a rate of €1,200 excl. VAT per person per day.

## 4. INSURANCE

Throughout the Test, the Tester must hold, with a reputable insurer, **professional liability insurance** covering material and immaterial damage caused to Pennylane and to third parties, and **cyber insurance** covering crisis management, data restoration, notification costs and third-party business interruption.

Minimum cover: €1,000,000 per claim. Insurance limits are **not** a cap on the Tester's liability.

Valid certificates, expressly covering penetration testing and social engineering, must be attached to the request. **The Testing Provider must hold equivalent cover.** Missing or invalid certificates mean the Authorisation is refused or automatically lapses.

## 5. RULES OF CONDUCT

### 5.1. Strictly prohibited — even with an Authorisation

- **Denial of service** (DoS, DDoS), load, stress or saturation testing, mass fuzzing, or anything else likely to affect the availability or performance of the Solution.
- **Destructive or altering actions**: deleting, modifying, encrypting or corrupting data or configurations; creating or changing accounting entries, invoices, mandates, payees or payment orders; triggering emails, SMS or notifications to real users.
- **Any access to, or retention of, Third-Party Data.** If the Scope is accidentally crossed or Third-Party Data is reached, the Tester must stop immediately, not go further, keep nothing, and notify Pennylane (section 8).
- **Data export** beyond the strict minimum needed to evidence a finding (a redacted screenshot, a limited extract).
- **Persistence**: backdoors, hidden accounts, scheduled tasks, webshells, malware or implants; pivoting or lateral movement into Pennylane's internal infrastructure.
- **Brute force, credential stuffing, password spraying** or mass account enumeration, and the use of real credential lists obtained elsewhere.
- **Application-level spam**: mass emails, SMS, invitations, reminders, form or API calls, including through invoicing, dunning or support features.
- **Social engineering against Pennylane staff, subcontractors or providers**: phishing, vishing, smishing, physical intrusion, pretexting the support or sales teams, attempts to bypass support authentication.
- **Testing third-party components** outside Pennylane's control: hosting (AWS), payment services (Compte Pro / Swan), banking aggregators, connectors and compatible solutions, subcontractors and third-party vendors. These require the relevant third party's own authorisation and are excluded from Scope by default.
- **Anything outside the Test Window or the approved Scope**, and anything unlawful (including French Criminal Code articles 323-1 et seq., GDPR, professional secrecy and trade secrets).

### 5.2. Mandatory during the Test

- Test only on the **environment designated** by Pennylane (dedicated or staging environment where provided; otherwise production under reinforced conditions).
- Use only the **test accounts and datasets** provided or approved by Pennylane; never use real third-party personal data.
- Respect the technical limits in the Authorisation: request cap (5 req/s max), declared and fixed source IPs, identifying header and specific user-agent.
- **Log everything** (timestamps, source IPs, requests), keep the logs and hand them to Pennylane on request.
- Apply **proportionality and minimisation**: evidencing a vulnerability never justifies fully exploiting it.
- Keep a **contact reachable at all times** during the Test Window, able to stop the Test within **1 hour**.
- Restore the system to its original state and remove every artefact created.

### 5.3. Pennylane's right to block

Pennylane may at any time and without notice block IP addresses, activate countermeasures, suspend user accounts or suspend the Tester's right of use under the applicable contract. This gives rise to no compensation, does not count as downtime under the potential SLA and does not trigger SLA credits.

## 6. PHISHING SIMULATIONS AND AWARENESS CAMPAIGNS

### 6.1. Who may be targeted

Only the **Tester's own staff**, previously informed that an awareness programme exists. Targeting Pennylane staff, the Tester's own customers, users of other firms, or anyone outside the Tester is strictly prohibited.

### 6.2. Brand and domains

Using the Pennylane name, brand, logo, visual identity, email templates or interface look-and-feel is specifically subject to receiving the prior Authorisation, with the request specifying which assets may be used and for how long. Registering or using look-alike domains (typosquatting, pennylane-xxx.com, misleading subdomains) is prohibited. If any such domain exists, it must be taken down immediately and transferred or deleted at Pennylane's request. No email may spoof an @pennylane.com sender or suggest a Pennylane origin.

### 6.3. Content and conduct

No scenario may undermine people's dignity or use sensitive themes (health, dismissal, bonuses, disciplinary action, personal circumstances, tragic news). **Real Pennylane credentials must never be collected** — capture pages must not store submitted passwords (block client-side, or otherwise truncate / irreversibly hash and delete immediately). Staff must not be prompted to contact Pennylane support, report fraud to Pennylane or perform a real operation in the Solution. No active attachments (macros, executables, scripts) may transit through Pennylane channels. Any debrief page must state clearly that this is an internal exercise and that Pennylane is not its author.

### 6.4. Employment law and GDPR

The Tester alone is responsible for compliance towards its employees: prior information and consultation of employee representative bodies, prior collective information, no disciplinary or individual use of results, minimised and anonymised statistics, limited retention, entry in the record of processing and, where relevant, a DPIA. Pennylane is neither controller, joint controller nor processor for this processing.

### 6.5. What to tell Pennylane

The request must state: sending dates and times, message volume, the phishing platform provider, sending domains and addresses, sending IP ranges, a copy of each email template and landing page, and the escalation contact.

## 7. PERSONAL DATA

Tests must be designed and run so that **no real personal data is collected or otherwise processed**. Where that is technically impossible, the Tester applies strict minimisation and documents the processing.

The Tester is the controller for all data collected during the Test and is solely responsible for compliance (legal basis, information, data subject rights, non-EU transfers, security, sub-processing).

All data, logs, screenshots and interim deliverables must be encrypted in transit and at rest, hosted in the EU, and **deleted no later than 30 days** after the final report, with a certificate of destruction provided on request.

Any accidental access to Third-Party Data is a potential personal data breach and must be notified within 24 hours at the latest to both dpo@pennylane.com and security@pennylane.com.

## 8. NOTIFICATION AND FINDINGS

All notifications go to security@pennylane.com:

| Event | Notification deadline |
|---|---|
| Critical or major vulnerability found | Immediately, and within 24 hours |
| Access to or extraction of Third-Party Data (with dpo@pennylane.com) | Immediately, and within 24 hours |
| Incident, downtime, degradation or abnormal behaviour | Immediately |
| Scope or Test Window unintentionally exceeded | Immediately |
| Compromise of the Testing Provider's environment, tools or deliverables | Immediately, and within 24 hours |
| Full final report | 15 calendar days after the Test ends |

Findings are Pennylane's **confidential information and trade secrets**. The Tester and its Testing Provider must not exploit, replay, resell, publish or disclose them to third parties (including CERTs, bug bounty platforms, press, social media, research communities), nor use them commercially, without Pennylane's prior written approval. This obligation survives the Test by 5 years.

Pennylane remediates according to its own vulnerability management process and priorities. The Agreement creates no remediation, timing or performance commitment, and the Tester is entitled to no fee, bounty or reward for findings.

## 9. TESTER LIABILITY, BREACH AND RECHARGING

### 9.1. Full liability

The Tester is **solely and fully liable** for the Test and all of its direct and indirect consequences, **including where it is run by a Testing Provider**. The Tester guarantees compliance with the Agreement by its Testing Provider, subcontractors and staff, and answers for their acts as for its own. If the request for Authorisation is made by the Testing Provider directly to Pennylane on behalf of a client / partner of Pennylane, they are both jointly liable towards Pennylane.

### 9.2. Authorisation is not a discharge

Issuing an Authorisation does not validate the methodology, does not guarantee the absence of risk, does not transfer any liability to Pennylane, and **in no way releases** the Tester from liability for damage caused.

### 9.3. Breach of the Agreement = breach of the main contract

If the Tester is a client or partner of Pennylane, any failure to comply with the Agreement is a **material breach** of existing standard terms of specific contract with Pennylane, entitling Pennylane — without prior formal notice and without prejudice to damages — to suspend the Tester's and its users' right of use immediately, stop the Test and block access, terminate the main contract at the Tester's exclusive fault, notify the competent authorities (CNIL, ANSSI/CERT-FR, ACPR, judicial authorities) and bring civil or criminal proceedings.

### 9.4. Recharging as of right

Where the Test causes damage, disruption or cost — **including where the Test was duly authorised** — Pennylane may recharge the Tester, as of right and against an itemised statement, for all costs incurred, including: time spent by Pennylane teams (Security, Infrastructure, Engineering, Support, Legal, Communication) at **€1,200 excl. VAT per person per day**, uplifted by **50%** outside business hours; on-call, crisis management, data and system restoration, and excess infrastructure or licence consumption; technical expertise, audit, forensics and external advice; legal, notification and communication

costs; compensation, credit notes, SLA credits or damages owed to third parties; and any fines or penalties imposed by an authority as a result of the Test.

### 9.5. Collection

These amounts are **due on receipt of invoice**. Late payment triggers the interest and fixed recovery indemnity provided in the applicable contract (if any) and by law.

If the Tester is a client or partner of Pennylane, it expressly authorises Pennylane to collect them by direct debit under the existing SEPA mandate and/or by set-off against any sum owed by Pennylane, without the Tester being able to object or raise any defence of non-performance.

### 9.6. Indemnity

The Tester indemnifies and holds harmless Pennylane, its officers, employees and subcontractors against any third-party claim, action or proceeding arising in whole or in part from the Test.

### 9.7. Caps

Any liability cap stated in the standard terms or a specific contract for the Tester's benefit do not apply to obligations arising under this Agreement.

## 10. CONFIDENTIALITY

The existence, content and results of the Test are confidential. No external communication (website, social media, tenders, conferences, research publications, commercial references) may refer to them without Pennylane's prior written approval. The Testing Provider must be bound by an at least equivalent confidentiality undertaking, a copy of which is provided on request.

## 11. AGREEMENT DURATION AND CHANGES

The Agreement applies from the date of the authorisation request until the confidentiality and liability obligations it contains expire. Pennylane may amend it at any time without notifying the clients, partners and previous Testers; the applicable version is the one in force when the request is submitted.

## 12. GOVERNING LAW AND JURISDICTION

This Agreement is subject to French law. Any dispute relating in particular to the validity, interpretation, or execution of the Agreement will be subject to the exclusive jurisdiction of the Commercial Court of Paris.

**Annex A – Request checklist**

- [ ] Tester details, Pennylane account and authorised signatory
- [ ] Operational contact reachable throughout the Test Window (phone + email)
- [ ] Detailed description of the Test (objectives, methodology, framework, tools, scenarios)
- [ ] Scope included / excluded (URLs, APIs, apps, accounts, environments)
- [ ] Dates, hours and time zone
- [ ] Volume and intensity (req/s, number of accounts, number of emails)
- [ ] Expected impact and mitigation measures
- [ ] Emergency stop procedure and response time
- [ ] Data collected: nature, personal or not, purpose, retention, deletion, DPIA
- [ ] Testing Provider identity, certifications, named testers, source IPs, signed NDA
- [ ] Insurance certificates for both Tester and Testing Provider
- [ ] Phishing only: target population, email templates, landing pages, domains, sender addresses, brand use, proof of employee/works council information

🚫 **Never**: DDoS or load testing · destroying or altering data · accessing other clients' data · exfiltration · persistence, backdoors or malware · brute force and credential stuffing · email, SMS or API spam · social engineering Pennylane staff · testing third-party components (AWS, Swan, banking aggregators, connectors) · acting outside Scope or Test Window · publishing or sharing results.

✅ **Always**: prior written approval · stay within Scope and Test Window · declared IPs and identifying header · test accounts and test data · capped request rate · full logging · immediate stop on request · notification within 24 hours · report shared with Pennylane · data deleted with certificate of destruction.