

FREE RESOURCE — PENETRATION TESTING

Penetration Test Preparation Checklist

Everything to lock down in the week before a penetration test starts — authorisation and legal sign-off, a frozen scope, verified backups, monitoring decisions, stakeholder communications, emergency contacts and evidence handling. Skip any of these and test week gets a lot more stressful than it needs to.

8

PREPARATION
AREAS COVERED

35+

PRE-TEST
CHECKS
TO TICK

7

DAYS BEFORE —
RECOMMENDED
LEAD TIME

Fillable

TICK & TYPE
IN ANY VIEWER

AUTHORISATION

BACKUPS

MONITORING

COMMS

PREPARED FOR

Cloudswitched Knowledge
Library

PREPARED BY

Cloudswitched Ltd.

VERSION

2026 Edition

FORMAT

Interactive PDF

01

Authorisation, scope & backups

Nothing starts without written authorisation. Confirm the paperwork, freeze the scope so the quote matches what actually gets tested, and verify your safety net is in place before anyone starts probing live systems.

Authorisation & legal sign-off

- **Signed authorisation letter / rules of engagement** is in place, naming the tester, the dates and the exact scope — before any testing begins.
- **Third-party consent obtained** for any in-scope asset you do not own outright (hosting provider, SaaS vendor, cloud platform terms of service).
- **Contract and NDA** are signed and filed; liability and indemnity clauses have been read by whoever owns the risk decision.
- **Insurer notified** if the policy requires advance notice of security testing activity.

Scope freeze

- **Final scope document** matches the quote — IP ranges, URLs, apps, exclusions — with no last-minute additions.
- **No planned changes** to in-scope systems during the test window (deployments, migrations, firewall changes) unless explicitly agreed.
- **Test credentials prepared** (if authenticated testing is in scope) — standard user, and if agreed, privileged accounts.

Backups verified

- **Full backup completed and verified restorable** for every in-scope system within 48 hours of test start.
- **Change freeze** on backup schedules during the test window, so a restore point always exists if something goes wrong.

ACTIVE TESTING CAN BREAK FRAGILE SYSTEMS

Even a professional, careful tester can crash a legacy application that was never built to handle unexpected input. A verified, restorable backup taken in the 48 hours before testing starts is non-negotiable — not a nice-to-have.

02

Monitoring, comms & evidence handling

Decide in advance whether your SOC should see the test coming, who needs to know it is happening, who to call if something breaks, and how the findings will be stored once the report lands.

Monitoring & alert whitelisting

- **Decision made and documented:** test the SOC's detection capability (no whitelisting) or whitelist tester IPs to avoid alert fatigue — not both by accident.
- **SOC / MSSP notified on-call** of test dates and tester source IPs, even if not whitelisted, to avoid a false real-incident response.
- **WAF / IPS blocking thresholds reviewed** so the test is not silently blocked before it produces useful findings.

Stakeholder communications plan

- **Leadership briefed** on dates, scope and expected disruption (if any); sign-off obtained to proceed.
- **IT / helpdesk briefed** so unusual traffic or user reports during the window are correctly triaged, not treated as a live incident.
- **Communication is need-to-know** — wide staff announcements can skew results if social engineering is in scope.

Emergency contacts & test-window agreement

TESTER EMERGENCY CONTACT

INTERNAL ON-CALL CONTACT

AGREED TEST WINDOW (DATES)

STOP-WORK / STAND-DOWN PHRASE

Evidence handling

- **Secure delivery channel agreed** for the report and any raw evidence (encrypted portal, PGP, password-protected archive).
- **Retention and deletion terms** for tester-held evidence, credentials and scan data are confirmed in the contract.



Final readiness sign-off

Tick every box on the previous two pages before the agreed start date. If anything is outstanding, move the date — starting a test with an unverified backup or no emergency contact is the wrong trade-off.

PREPARATION CHECKS COMPLETE

/ 14

All 14 must be ticked before test start.

Outstanding items & notes

Sign-off

READINESS CONFIRMED BY

ROLE / TITLE

DATE

Booking a test and want the prep handled?

Cloudswitched manages the full pre-test process for clients — authorisation, scope freeze, backup verification and stakeholder comms — alongside the test itself.

info@cloudswitched.com

cloudswitched.com/services/penetration-testing



CLOUDSWITCHED

OPTIMIZE YOUR IT AND THRIVE

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom