Amethyst Cyber Group
Common Sense Cyber Security

CLIENT CONFIDENTIAL

PREREQUISITES CHECKLIST

Penetration Testing Prerequisites

Information and access required before a penetration test engagement begins.

CLIENT **[Client Organisation]**	DOCUMENT REF **ACG-PRE-PT**
VERSION **2.0**	ISSUED **June 2026**

Purpose. Complete this checklist before the engagement start date. Return completed items to your Amethyst Cyber Group project contact. Do not send credentials or production secrets by email — use the agreed secure channel.

Penetration Testing Prerequisites

Complete all sections relevant to your scope. Tick each item when the information has been provided or confirmed.

General — All Engagements

- [ ] Provide a named project contact, technical escalation contact, and emergency stop contact with direct phone numbers before testing starts.
- [ ] Confirm agreed test windows (start date, end date, daily hours), out-of-hours restrictions, and any change freeze periods.
- [ ] Confirm the testing approach: black box (no prior knowledge), grey box (partial documentation and credentials), or white box (full documentation, source access, and credentials).
- [ ] Confirm any systems, hosts, or IP ranges that are explicitly out of scope and must not be tested.
- [ ] Confirm IP allow-listing requirements — provide Amethyst Cyber Group source IPs to firewall and WAF teams before testing begins.
- [ ] Confirm MFA arrangements for test accounts: how bypass or enrolment will be handled without disrupting production users.
- [ ] Confirm evidence handling expectations: encryption requirements, storage location, and retention or deletion timeline for captured evidence.
- [ ] Confirm whether the internal security team, SOC, or monitoring platform should be notified of the test — and if so, who is the single point of contact.
- [ ] Do not send production secrets, credentials, or private keys by email. Use the agreed secure channel (e.g., password manager share link, encrypted transfer).

Web Application Testing

- [ ] Provide a complete list of all in-scope target URLs, domains, and subdomains, including any staging or test environments to be used.
- [ ] Provide test accounts for every application role in scope (e.g., unauthenticated, standard user, privileged user, admin, super-admin, API consumer).
- [ ] Provide API documentation (Swagger / OpenAPI spec, Postman collection, or equivalent) where the application has API-backed workflows.
- [ ] Identify business-critical or fragile workflows (e.g., payment flows, data deletion, user provisioning) that require extra care or prior agreement before testing.
- [ ] Confirm rate limiting thresholds, WAF rules, CAPTCHA, and bot protection in place — and whether WAF bypass mode is available for testing.
- [ ] Confirm whether third-party integrations (payment gateways, SSO providers, external APIs) are in scope or explicitly excluded.
- [ ] Confirm whether single sign-on (SSO/SAML/OIDC) is in scope and provide test credentials or an agreed bypass mechanism.
- [ ] Provide test data for file upload, form submission, and input validation testing — ensure test data does not contain real personal data.

- [ ] Confirm whether multi-tenant functionality is in scope and provide accounts across multiple tenants if applicable.

API Testing

- [ ] Provide the full API specification: OpenAPI / Swagger, Postman collection, GraphQL schema, or equivalent documentation.
- [ ] Confirm the API type(s) in scope: REST, GraphQL, gRPC, SOAP, or a combination.
- [ ] Provide authentication material including API keys, OAuth 2.0 client credentials, token endpoints, JWT details, and token refresh flows.
- [ ] Provide test credentials for all API roles and permission levels (e.g., read-only, read-write, admin, service account).
- [ ] Confirm all versioned endpoints and identify any deprecated or internal routes that are in scope.
- [ ] Confirm rate limits, throttling policies, and IP restrictions applied to API calls — and whether test traffic requires exemption.
- [ ] Identify webhooks, callbacks, asynchronous operations, and event-driven routes within scope.
- [ ] Confirm whether direct API access is authorised or whether testing should replicate client (mobile / web) traffic patterns only.

Mobile Application Testing

- [ ] Provide test builds: iOS (IPA) and / or Android (APK) — debug builds are strongly preferred to allow deeper runtime analysis.
- [ ] Confirm supported OS versions, minimum deployment targets, and any device or jailbreak / root constraints.
- [ ] Provide test accounts for all backend user roles accessible from the mobile application.
- [ ] Provide backend API base URLs and environment details — confirm whether a dedicated test environment is available.
- [ ] Confirm whether certificate pinning is implemented and whether bypass is permitted during testing.
- [ ] Confirm MDM or enterprise certificate constraints that affect sideloading or installing test builds on test devices.
- [ ] Provide details of deep link handling, custom URL schemes, and any inter-app communication mechanisms in scope.
- [ ] Confirm whether in-app purchase, payment, or subscription flows are in scope — if so, provide test payment credentials.
- [ ] Confirm whether biometric authentication is used and how it should be handled during runtime testing.

External Infrastructure Testing

- [ ] Provide a complete list of in-scope external IP addresses and CIDR ranges — confirm all are under the client's ownership and control.
- [ ] Provide all in-scope hostnames and domains, including any subdomains that should be included in enumeration.
- [ ] Confirm whether subdomain enumeration beyond the provided list is permitted.
- [ ] Identify any CDN, DDoS mitigation, load balancer, or WAF in front of target systems, and provide the real IP if allow-listing is required.
- [ ] Confirm maintenance windows and any time-of-day restrictions (e.g., no scanning during peak business hours).
- [ ] Identify fragile, legacy, or OT-adjacent systems requiring reduced scan intensity or explicit pre-authorisation before probing.
- [ ] Provide ASN, netblock, or BGP routing information for large or complex external estates.
- [ ] Confirm whether remote access services (VPN portals, RDP gateways, Citrix, Pulse Secure) are in scope.

Internal Infrastructure Testing

- [ ] Provide CIDR ranges for all in-scope internal networks, including any isolated segments, OT VLANs, or DMZs.
- [ ] Confirm the starting position for testing: assumed breach (foothold already established), authenticated domain user, or unauthenticated.
- [ ] Provide Active Directory forest name(s), domain name(s), and domain controller IP addresses.
- [ ] Provide a test domain account with standard user privileges if authenticated testing is agreed — confirm account will not expire during the test window.
- [ ] Identify critical infrastructure that requires extra care or is explicitly excluded: domain controllers, backup systems, OT / ICS, SCADA, CCTV, and telephony.
- [ ] Confirm VPN or on-site access arrangements, including hardware drop box or agent-based access if no VPN is available.
- [ ] Provide VLAN layout, segmentation boundaries, and firewall between-zone rules where available.
- [ ] Confirm whether Defender for Identity, EDR, or SIEM is active and whether the blue team should be notified (white team exercise vs. blind test).
- [ ] Confirm network diagrams or topology documents — these remain confidential and support safe testing only.

Cloud Testing

General cloud prerequisites

- [ ] Confirm cloud provider(s) in scope: Azure, Microsoft 365, AWS, Google Cloud, Oracle Cloud, or combination.
- [ ] Provide tenant ID, subscription ID, account ID, or project ID for each in-scope cloud environment.

- [ ] Provide a test identity (service principal, IAM user, or agreed role) with appropriate permissions for the agreed scope.
- [ ] Confirm testing scope: identity and IAM review, storage and data plane, networking and firewall rules, workload security, logging and detection, or full-scope.
- [ ] Confirm guardrails that must not be crossed: no deletion of resources, no exfiltration of production data, no cost-generating actions without pre-approval.
- [ ] Provide logging contact or SIEM team who should be notified of test activity to avoid false-positive incident response.

Azure / Microsoft 365

- [ ] Provide Entra ID (Azure AD) tenant ID and confirm whether guest / B2B accounts are in scope.
- [ ] Confirm M365 workloads in scope: Exchange Online, SharePoint, Teams, OneDrive, Intune, Defender for M365, or Entra ID.
- [ ] Confirm whether Conditional Access policies are in place and how test accounts will satisfy or bypass them.
- [ ] Confirm whether multi-tenant or shared-tenant constraints apply (e.g., partner tenants, group company co-tenancy).

AWS

- [ ] Provide AWS account ID(s), region(s) in scope, and confirm whether AWS Organizations / Control Tower is used.
- [ ] Provide an IAM user or role with agreed permissions — confirm SCP guardrails that restrict test identity actions.
- [ ] Note: AWS penetration testing does not require prior notification to AWS for supported services, but confirm any third-party services hosted on AWS that may be out of scope.

Google Cloud

- [ ] Provide project IDs, organisation ID, and folder structure where relevant to scope.
- [ ] Provide a service account or test identity with agreed IAM roles — confirm organisation policy constraints.

Wireless Testing

- ☐ Provide site address(es) and, where available, floor plans or physical layout to help plan antenna placement.
- ☐ Confirm all SSIDs in scope: corporate, guest, IoT, management, and any hidden networks.
- ☐ Confirm whether SSID enumeration and passive rogue AP detection is authorised beyond the provided list.
- ☐ Provide wireless authentication details: WPA2-PSK, WPA3, WPA2-Enterprise (RADIUS, EAP type), or captive portal.
- ☐ Provide pre-shared keys or RADIUS test credentials where authenticated testing is agreed.
- ☐ Confirm physical access arrangements and operating hours for the site visit.
- ☐ Identify sensitive areas where wireless testing activity (antennas, laptops) may cause concern: server rooms, trading floors, clinical areas.
- ☐ Confirm whether wired network access is available for test equipment such as a laptop or wireless bridge.
- ☐ Identify any wireless-connected OT, medical, or safety-critical devices that are explicitly excluded from testing scope.

Physical Penetration Testing

> **Mandatory.** A signed Letter of Attestation must be received before any physical testing begins. Use the ACG Physical Testing Letter of Attestation template.

- ☐ Provide site address(es), permitted testing dates and times, and site operating hours.
- ☐ Provide a dedicated emergency stop contact with a direct phone number and authority to immediately pause testing at any time.
- ☐ Provide security desk, reception, and facilities contact details for use if a tester is challenged on-site.
- ☐ Confirm permitted areas (e.g., reception, open-plan office, server room) and explicitly prohibited areas (e.g., executive suites, data centres without escort).
- ☐ Confirm permitted techniques: tailgating, social engineering, physical lock bypass, door hardware bypass, RFID cloning, access control analysis.
- ☐ Confirm prohibited techniques: destructive entry, forcing locks, damaging property, or any technique requiring explicit additional sign-off.
- ☐ Confirm the testing approach: covert (security staff unaware), overt (security staff fully briefed), or hybrid (reception aware, security staff unaware).
- ☐ Confirm whether on-site CCTV, access control, or alarm systems will record test activity — and whether this is treated as evidence.
- ☐ Confirm what procedure applies if a tester is detained, challenged, or stopped by security or police during the exercise.
- ☐ Confirm whether physical testing is standalone or embedded within a red team engagement, and how deconfliction with cyber activity is managed.
- ☐ Provide a signed Letter of Attestation before testing begins — unsigned attestation is not sufficient to authorise physical access.

Evidence and Reporting

- [ ] Confirm report classification and distribution: who receives the final report, and whether a separate executive summary is required.
- [ ] Confirm retest requirements: whether a retest window is needed to validate remediation of critical or high findings.
- [ ] Confirm evidence destruction timeline: when screenshots, tool output, and captured data should be securely deleted after the engagement closes.