Amethyst Cyber Group
Common Sense Cyber Security

CLIENT CONFIDENTIAL

PREREQUISITES CHECKLIST

Red Team Prerequisites

Information, authorisations, and access required before a red team engagement begins.

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

Important. Red team engagements require extensive pre-engagement planning. All sections must be completed and signed-off before the engagement start date. Do not send credentials or sensitive material by email.

Red Team Prerequisites

Red team engagements are objective-led and adversarial in nature. Complete all sections before work begins. The trusted contact group must be kept strictly confidential — do not share the engagement with IT, security teams, or staff unless they are named in the white cell.

Contacts and Trusted Group

- [ ] Define the white cell — the small group of authorised individuals who are aware of the engagement. Names and roles must be confirmed in writing before work begins.
- [ ] Provide a named executive sponsor with authority to authorise the engagement and make stop / go decisions.
- [ ] Provide a dedicated emergency stop contact with a direct mobile number, available at any time during the engagement window.
- [ ] Confirm the deconfliction process: how the red team contacts the white cell if an activity risks causing a real incident or business disruption.
- [ ] Confirm daily or regular check-in cadence and the communication channel to be used (e.g., encrypted messaging, dedicated email).
- [ ] Do not involve the SOC, IT team, or security operations staff unless they are explicitly named in the white cell.

Objectives and Scope

- [ ] Define primary and secondary objectives — the specific outcomes the engagement is designed to test (e.g., reach domain admin, exfiltrate a defined file, gain access to a named system).
- [ ] Identify crown jewels: the systems, data, or processes that represent the most sensitive targets in scope.
- [ ] Confirm the engagement model: assumed breach (initial foothold provided), external initial access only, or full-chain from external reconnaissance.
- [ ] Confirm the threat profile: generic opportunistic attacker, nation-state-level TTPs, financially motivated actor, or a named threat group to emulate.
- [ ] Confirm systems and techniques that are explicitly out of scope — including any systems that must never be targeted under any circumstances.
- [ ] Confirm whether destructive techniques are permitted (e.g., disabling accounts, modifying data) or whether read-only / non-destructive TTPs are required.

Technical Access and Infrastructure

- [ ] For assumed breach engagements: confirm how the initial foothold will be established — implant delivered by ACG, pre-staged credentials, or a test user account.
- [ ] Provide asset documentation in scope: IP ranges, domain names, cloud tenant IDs, VPN endpoints, and known perimeter services.
- [ ] Confirm whether Active Directory, cloud identity (Entra ID / AWS IAM / GCP IAM), or both are in scope for lateral movement and privilege escalation testing.

- [ ] Confirm VPN or network access method if testing includes internal infrastructure segments not reachable from the internet.
- [ ] Confirm whether logging and detection infrastructure (SIEM, EDR, NDR) is active during the engagement — this is expected, and part of what will be tested.
- [ ] Do not send credentials, VPN configs, or access material by email. Use the agreed secure channel.

Social Engineering Scope

- [ ] Confirm whether phishing simulation is in scope and the permitted approach: generic credential-harvest, targeted spear-phishing, or pretexted business email.
- [ ] Confirm whether phone-based vishing or smishing is permitted, and any restrictions on impersonation of real individuals or brands.
- [ ] Confirm whether physical social engineering (tailgating, impersonation on-site) is included — if so, refer to the Physical Scenarios section below.
- [ ] Confirm any employee groups or individuals who must not be targeted (e.g., executives, HR, legal, individuals on leave or medical absence).
- [ ] Confirm the notification process if an employee reports a phishing or social engineering attempt during the engagement.
- [ ] Confirm whether phishing infrastructure should simulate a real supplier, partner, or internal IT team, and the boundaries on domain spoofing and brand impersonation.

Physical Scenarios

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

- [ ] Provide site address(es), permitted testing dates and times, and operating hours for each site.
- [ ] Provide emergency stop contact with a direct phone number and authority to pause physical activity immediately.
- [ ] Provide security desk, reception, and facilities contact details for use if a tester is challenged on-site.
- [ ] Confirm permitted areas, prohibited areas, and permitted techniques for each site.
- [ ] Confirm whether the physical scenario is covert (security unaware), overt (security briefed), or hybrid.
- [ ] Confirm the procedure if a tester is detained, challenged, or stopped by security or police during the exercise.
- [ ] Provide a signed Letter of Attestation before any physical activity begins.

Evidence, Reporting, and Closure

- [ ] Confirm evidence retention policy: all captured data, screenshots, and tool output must be stored securely and deleted after the agreed retention period.
- [ ] Confirm what happens at the end of the engagement: full cleanup of implants, persistence mechanisms, created accounts, and any modified configurations.
- [ ] Confirm report classification and distribution: the final report is highly sensitive and its distribution must be agreed with the white cell before delivery.

- [ ] Confirm whether a debrief workshop is required, and whether the blue team should be included in a post-engagement purple team session.