CLIENT INTAKE QUESTIONNAIRE

Red Team / Physical Security Assessment

Please complete all sections. Fields marked with * are required. This information will be used to scope your engagement.

1. CLIENT INFORMATION

Organization Name *

Industry / Sector *

Primary Contact Name *

Title / Role

Email Address *

Phone Number *

Secondary Contact Name

Secondary Phone

Physical Address (Headquarters) *

Mailing Address (if different)

2. FACILITY INFORMATION

Number of Facilities to be Assessed *

Facility Address(es) — List all locations to be included in scope

Facility Type(s)

- [ ] Corporate Office
- [ ] Data Center
- [ ] Warehouse
- [ ] Manufacturing
- [ ] Retail
- [ ] Healthcare
- [ ] Other

Approximate Square Footage

Number of Floors

Normal Business Hours

24/7 Operations?

3. ENGAGEMENT GOALS & COMPLIANCE

What prompted this assessment? *

- [ ] Compliance Requirement
- [ ] Audit Preparation
- [ ] Security Incident
- [ ] Proactive Testing
- [ ] Insurance Requirement
- [ ] Executive Request
- [ ] New Facility
- [ ] Other

If compliance-driven, select applicable framework(s):

- [ ] PCI-DSS
- [ ] HIPAA
- [ ] SOC 2
- [ ] ISO 27001
- [ ] NIST 800-53
- [ ] NIST CSF
- [ ] FedRAMP
- [ ] CMMC
- [ ] GLBA
- [ ] NERC CIP
- [ ] State Privacy Law
- [ ] Other

Specific compliance controls or requirements to be tested:

Auditor / Assessor Name (if applicable)

Audit Deadline

Previous audit findings to retest or validate:

4. SCOPE PARAMETERS

Assessment Types Requested (check all that apply) *

- [ ] Physical Penetration
- [ ] Social Engineering (In-Person)
- [ ] Phishing/Email Pretext
- [ ] Wireless/WiFi Testing
- [ ] Network Penetration
- [ ] Web Application
- [ ] USB Drops/Implants
- [ ] Full Red Team

Testing Approach

- [ ] Black Box (No Info)
- [ ] Gray Box (Limited Info)
- [ ] White Box (Full Info)
- [ ] Assumed Breach

Primary Objectives — What do you want to learn or validate? *

Are any locations, areas, or systems explicitly OFF-LIMITS? *

5. TECHNICAL / CYBER SCOPE

External IP Ranges / Domains in Scope:

Internal IP Ranges in Scope (if applicable):

Wireless Networks (SSIDs) in Scope:

Cloud Environments in Scope:

☐ AWS ☐ Azure ☐ GCP ☐ Other Cloud ☐ None

Will test credentials or accounts be provided? (for assumed breach)

☐ Yes ☐ No ☐ TBD

If yes, describe access level and account types:

Sensitive or fragile systems to avoid or handle carefully:

Is the SOC/NOC aware of this engagement?

☐ Yes - Full Awareness ☐ Yes - Limited Awareness ☐ No - Testing Detection ☐ TBD

6. TECHNICAL POINTS OF CONTACT

IT Emergency Contact (Name / Phone / Email)

SOC/NOC Contact (Name / Phone / Email)

Facilities Contact (Name / Phone / Email)

7. AUTHORIZATION & LEGAL

Who has authority to authorize this assessment? *

Property Ownership

☐ Owned ☐ Leased ☐ Shared/Co-located ☐ Multiple Tenants

If leased or shared, third parties requiring authorization or notification:

Will law enforcement be pre-notified?

☐ Yes ☐ No ☐ To Be Determined

8. CURRENT SECURITY POSTURE

Existing Physical Security Measures (check all that apply)

☐ Security Guards ☐ CCTV/Cameras ☐ Badge Access Control
☐ Biometrics ☐ Mantrap/Airlock ☐ Alarm System
☐ Perimeter Fence ☐ Visitor Mgmt System ☐ K9 Units

Have you had a security assessment before?

☐ Yes - Physical ☐ Yes - Cyber/Pentest ☐ Yes - Both ☐ No

Key findings or areas of concern from previous assessments:

9. CONSTRAINTS & SCHEDULING

Desired Start Date

Desired End Date

Blackout Dates/Windows (dates or times when testing cannot occur):

Budget Range (if known)

Decision Timeline

10. ADDITIONAL INFORMATION

Any other information, concerns, or questions?

Submitted By (Print Name)

Date