SENTINEL SAFEGUARD LLC

Security For Everyone | Kansas City, MO | 816-533-8418 | Sentinelsafeguard@outlook.com

PENETRATION TESTING AUTHORIZATION AND RULES OF ENGAGEMENT

TEMPLATE — NOT LEGAL ADVICE. *This instrument was synthesized from industry practice, including PTES pre-engagement guidance and SANS/OWASP engagement norms. It is not legal advice and creates no attorney–client relationship.* ***Have a Missouri business attorney review this Authorization before first client use — this is non-negotiable*** *— and again whenever you take on a new category of test (physical intrusion, wireless, social engineering).*

NO TESTING OF ANY KIND BEGINS UNTIL THIS DOCUMENT IS SIGNED BY BOTH PARTIES. *Keep a signed copy accessible for the duration of the engagement. If any person questions your presence or activity on Client systems, this document is your authority to act.*

RECITALS

This Penetration Testing Authorization and Rules of Engagement (this "Authorization") is entered into as of the Effective Date set forth below, by and between Sentinel Safeguard LLC, a Missouri limited liability company with its principal place of business in Kansas City, Missouri ("Provider"), and the undersigned client ("Client").

WHEREAS, Client desires to engage Provider to conduct authorized penetration testing and related security assessment activities against Client's systems; and

WHEREAS, the Parties wish to define with precision the scope, methods, timing, and rules governing such testing, so that all testing is conducted lawfully and with Client's informed consent;

NOW, THEREFORE, Client hereby authorizes Provider, through its designated tester(s), to perform the security testing described herein, strictly within the scope, windows, and rules set forth below.

PARTIES AND EFFECTIVE DATE

Effective Date — the date this Authorization is signed, MM/DD/YYYY. No testing is authorized before this date.

Engagement ID — Sentinel-assigned reference, format ENG-YYYY-####. Must match the SOW.

Client full legal name — the registered legal name as filed with the state. Do not use a DBA or trade name.

Provider: Sentinel Safeguard LLC, Kansas City, MO — Skyler Henderson, President & Lead Director of Operations — 816-533-8418 — Sentinelsafeguard@outlook.com.

SECTION 1 — GRANT OF AUTHORIZATION

1.1 **Explicit grant.** Client expressly authorizes Provider and its designated tester(s) to perform the security testing described herein against the targets in Section 2, during the windows in Section 3, using only the techniques permitted in Section 4. 1.2 **Scope limitation.** This Authorization extends only to the listed targets, windows, and techniques. Any activity outside them is not authorized. 1.3 **Non-transferable.** This Authorization is specific to the

Parties and the engagement identified above and may not be transferred or relied upon by any third party.

SECTION 2 — SCOPE

2.1 In-scope targets

Only the targets below are authorized. **If it is not listed here, do not touch it.**

#	Target	Type	Notes
1	*IP, range, domain, or system — exact*	*Type — external, web app, internal, wireless, physical*	*Notes — test accounts, on-site/VPN, handling*
2	*IP, range, domain, or system*	*Type*	*Notes*
3	*IP, range, domain, or system*	*Type*	*Notes*
4	*IP, range, domain, or system*	*Type*	*Notes*

2.2 Explicitly out of scope

The following are expressly excluded and shall not be tested, scanned, or accessed:

Out-of-scope system — exact description, e.g. "Production payment database cluster (prod-db-01/02)", "Office 365 tenant", "Employee personal devices."

Out-of-scope system — exact description. Be specific.

2.3 Third-party systems

Any target owned or operated by a party other than Client — including hosting providers, ISPs, and cloud vendors (e.g., AWS, Azure, Google Cloud) — may be tested **only** if Client has obtained that third party's written permission **before** testing begins and has provided a copy to Provider. **Provider shall not test third-party infrastructure without such permission.** Client's authorization alone is insufficient for systems Client does not own.

SECTION 3 — AUTHORIZED TESTING WINDOWS

Item	Detail
Testing window	_____ *Days and hours — e.g. "Mon–Fri, 6:00 PM – 6:00 AM America/Chicago"*
Blackout periods	_____ *No testing — e.g. month-end close, holidays, launch dates*
Engagement start date	_____ *First date testing may occur — MM/DD/YYYY*
Engagement end date	_____ *Last date testing may occur — MM/DD/YYYY*

Testing outside these windows, or after the end date, is not authorized unless both Parties agree in writing.

SECTION 4 — AUTHORIZED TECHNIQUES

_____

Permitted techniques — list every one, e.g. "Network scanning, vulnerability scanning, manual web application testing, password guessing against provided test accounts only, privilege escalation and lateral movement within scope."

_____

_____

_____

The following are **prohibited** without separate prior written approval from Client: denial-of-service (DoS/DDoS) testing of any kind; intentional destruction, corruption, or deletion of data; testing of any system not listed in Section 2.1; social engineering of Client personnel (unless expressly permitted above); physical intrusion, lock bypass, or tailgating (unless a physical test is in scope); introduction of persistent malware, ransomware, or backdoors; exfiltration of real customer or personal data — proof of access only (e.g., directory listing, file count), then stop immediately.

SECTION 5 — EMERGENCY CONTACTS AND STOP-WORK

5.1 Contacts

Role	Name	Phone	Email	Availability
Client primary contact	_____ *Full name*	_____ *Phone*	_____ *Email*	_____ *Hours*
Client escalation (24/7)	_____ *Full name*	_____ *Phone*	_____ *Email*	24/7 during testing

Role	Name	Phone	Email	Availability
Provider lead	Skyler Henderson	816-533-8418	Sentinelsafeguard@outlook.com	During testing windows

5.2 Stop-work procedure

Either Party may order an **immediate stop** to all testing at any time, for any reason, by telephone or email to the contacts above. Upon receiving a stop order, Provider shall cease all testing within fifteen (15) minutes and confirm cessation in writing. Testing resumes only upon the written agreement of both Parties. Agreed stop-word for urgent telephone calls:

Stop-word — one codeword, e.g. "REDLIGHT". When Client speaks this word on a call, testing stops immediately, no questions asked.

SECTION 6 — IF SOMETHING BREAKS

If Provider causes or discovers a system outage, data corruption, or service degradation: (a) Provider stops the activity immediately; (b) Provider notifies the Client primary contact within fifteen (15) minutes; (c) the Parties cooperate on recovery before any testing resumes. Provider shall exercise professional care to avoid disruption; Client acknowledges adversarial testing carries inherent risk despite such care (see Section 11).

SECTION 7 — REAL INCIDENTS DISCOVERED DURING TESTING

If Provider discovers evidence of an actual ongoing attack, intrusion, or breach not caused by the test: (a) Provider notifies the Client primary contact immediately — this takes priority over the test; (b) Provider preserves evidence and documents findings without contaminating the scene; (c) further action follows Client's incident response plan, and testing is paused until Client directs otherwise in writing.

SECTION 8 — DATA HANDLING AND CONFIDENTIALITY

8.1 All credentials, data, and findings obtained during the engagement are Client's Confidential Information. 8.2 Provider shall store engagement data encrypted and access-controlled, retaining it for ninety (90) days after the final report unless Client directs otherwise in writing. 8.3 Upon expiration of the retention period, Provider shall securely destroy all Client data per NIST SP 800-88 and confirm destruction in writing upon request. 8.4 Provider shall not disclose vulnerabilities or findings to any third party without Client's prior written permission.

SECTION 9 — REPRESENTATIONS AND WARRANTIES

9.1 Client represents and warrants that (a) it owns, controls, or has the owner's written permission for every system in Section 2.1; (b) it has obtained all third-party permissions required by Section 2.3; and (c) the individual executing this Authorization has full power and authority to grant the permissions herein on Client's behalf. 9.2 **An individual who signs without such authority may be held personally liable.** If in doubt, obtain written authorization from Client's ownership or board before signing. 9.3 Provider represents that testing shall be performed with professional care, strictly within the authorized scope, windows, and techniques.

SECTION 10 — INDEMNIFICATION; HOLD HARMLESS

10.1 To the fullest extent permitted by law, Client shall indemnify, defend, and hold harmless Provider, its owner, officers, and personnel against claims, damages, losses, and reasonable attorneys' fees arising from testing performed within the authorization granted herein, except to the extent caused by Provider's gross negligence or willful misconduct. 10.2 Each Party shall indemnify the other for claims arising from the indemnifying Party's gross negligence, willful misconduct, or breach of this Authorization, including any misrepresentation under Section 9. 10.3 Client is responsible for notifying its IT staff, hosting providers, and insurers that authorized testing will occur, and for obtaining the third-party permissions required by Section 2.3.

SECTION 11 — LIMITATION OF LIABILITY

11.1 TO THE MAXIMUM EXTENT PERMITTED BY LAW, PROVIDER'S AGGREGATE LIABILITY UNDER THIS AUTHORIZATION SHALL NOT EXCEED THE FEES PAID FOR THE ENGAGEMENT. 11.2 NEITHER PARTY SHALL BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES. 11.3 Nothing here limits liability for gross negligence, willful misconduct, breach of confidentiality, or indemnification obligations, or liability that cannot be limited by law.

SECTION 12 — TERM; EXPIRATION; REVOCATION

12.1 This Authorization runs from the Effective Date through the engagement end date in Section 3, during the authorized windows only, and **expires automatically** at the end date without further action. 12.2 Either Party may revoke at any time by written notice; upon revocation, Provider ceases all testing within fifteen (15) minutes.

SECTION 13 — GENERAL PROVISIONS

13.1 **Entire agreement; amendments.** This Authorization, with the Engagement Letter and SOW, is the entire agreement regarding the testing described herein, amendable only by a signed writing of both Parties. 13.2 An unenforceable provision shall be narrowed to the minimum extent necessary; the remainder continues in full force. 13.3 Notices: email counts as written notice, effective upon receipt. Notices to Provider: Sentinelsafeguard@outlook.com. 13.4 Missouri law governs. Exclusive jurisdiction and venue lie in the state and federal courts of Jackson County, Missouri. 13.5 Counterparts; electronic signatures have the same force as handwritten signatures.

SIGNATURES

IN WITNESS WHEREOF, the Parties have executed this Authorization as of the Effective Date. **The Client signatory attests being duly authorized to grant permission to test the systems in scope on Client's behalf.**

	PROVIDER	CLIENT
Signature	*Sign in ink — Skyler Henderson*	*Sign in ink — individual authorized to bind Client*
Printed name	Skyler Henderson	*Print signatory's full legal name*
Title	President & Lead Director of Operations	*Title — must evidence authority to bind the company. See §9.2.*
Date	*MM/DD/YYYY*	*MM/DD/YYYY*