Authorization and Rules of Engagement

Savisa Security — authorized on-site security testing

Engagement ID: _____ Effective date: _____

Client: _____, a _____, with a principal place of business at _____ (city and state) (the **Client**, **you**, or **your**).

Provider: SavIsa Solutions LLC, a Michigan limited liability company doing business as Savisa Security, based in Shelby Twp, MI (**Savisa**, **we**, **us**, or **our**).

This Authorization and Rules of Engagement (this **Authorization**) is the Client's written permission for Savisa to perform the authorized security testing described below, and the rules both parties will follow. It is a contract. Please read it carefully. If you do not have authority to authorize testing of every in-scope system, do not sign it.

1. Scope and in-scope assets

Savisa may test only the assets listed in this section, and only in the ways this Authorization allows. Anything not listed here is out of scope.

The purpose of the work is: _____

In-scope assets (list each one: type; name or description; identifier such as IP, URL, hostname, SSID, device ID, or location; environment; and whether work is on-site, remote, or both):

_____

_____

In-scope physical locations (on-site work only): list a site name with city and state. A street address is not required on this public copy.

_____

In-scope testing methods (mark only what is authorized):

■ External network and service testing of listed addresses

■ Internal network testing from an agreed on-site point of presence

■ Wireless testing of listed SSIDs or access points, from agreed locations only

■ Application or web testing of listed URLs or applications

■ Configuration or credential review of listed systems, using accounts the Client provides

■ Other, limited to: _____

If a system, address, account, or location is discovered during the work and is not listed above, Savisa will not test it unless the Client first amends this Authorization in writing.

2. Ownership and authority attestation

The Client represents and warrants all of the following:

1. The Client is authorized to permit security testing of every in-scope asset.

2. The Client **owns**, or has a written right to authorize testing of, each in-scope asset.

3. If any in-scope asset is hosted, provided, or operated by a **third party** — including a cloud provider, data center, internet service provider, managed-service provider, landlord, co-tenant, parent, subsidiary, customer, or vendor — the Client has obtained that party's **prior written permission** for the testing described here, to the extent that party's terms or

the law require it, and will give Savisa a copy of that permission before testing of that asset begins.

4. The Client has the authority to grant Savisa access to the in-scope physical locations during the testing window, including any required visitor, escort, or after-hours arrangements.

5. The person signing this Authorization has authority to bind the Client.

6. The Client has identified, in writing, any in-scope system that is subject to a special legal or contractual limit (for example, a payment system, a system that holds medical or student records, or a system the Client does not fully control). Those limits are: _____ (or none).

The Client agrees to notify Savisa immediately if any of these statements becomes untrue, or if a third party withdraws permission, before or during the testing window. Savisa may pause or stop the work if it reasonably doubts that authority exists for an asset, until the Client provides satisfactory written confirmation.

3. Testing window and emergency contacts

Testing may occur only during the following period, in the local time of the in-scope location, unless both parties agree in writing to a change:

Start: _____ End: _____

Allowed hours (if narrower than the window): _____

On-site dates confirmed by the Client: _____

Savisa will not begin testing before the start of the window, and will stop at the end of the window, except for a controlled wind-down already in progress or a stop required by Section 5.

Emergency and day-to-day contacts. Complete name, title, and email before signature. Savisa will confirm its contacts when it countersigns. Contacts on this public copy are reached by email.

Client primary contact: name _____ title _____ email _____

Client technical contact: name _____ title _____ email _____

Client after-hours / emergency contact: name _____ email _____

Savisa primary contact: name _____ title _____ email _____

Savisa after-hours / emergency contact: name _____ email _____

How to reach each other in an emergency: by email to the emergency contact named above, and any secondary method the parties confirm in writing. The Client will have a person with authority available during testing hours to receive a stop notice and to make a decision about continuing, pausing, or ending the work.

4. Out-of-scope items and prohibited techniques

Out of scope. Unless this Authorization expressly lists them as in-scope, the following are out of scope: any system, network, account, cloud tenant, domain, device, or location not listed in Section 1; systems of the Client's customers, vendors, or partners; public or third-party infrastructure that is not owned or controlled by the Client and is not covered by a written third-party permission given to Savisa; denial-of-service testing, load testing intended to disrupt service, or bandwidth flooding; physical destruction, forced entry, or bypass of physical locks or alarms, unless a separate written authorization says otherwise; testing against personal devices of employees or visitors, unless a listed in-scope asset; social engineering, phishing, or pretexting of the Client's staff, customers, or vendors, unless a separate written authorization says otherwise; and any other client-specific exclusions: _____.

Prohibited techniques. Even on in-scope assets, Savisa will not: knowingly cause damage to hardware, or delete or encrypt data, except as needed for a brief, reversible test that the Client has approved in writing in advance; introduce ransomware, a wiper, or other malware that Savisa cannot reliably control or remove; exfiltrate, copy, or store more Client data than is reasonably necessary to demonstrate a finding, and will not take copies of data off the agreed work

location or systems except as Section 6 allows; use access obtained during the test to move into an out-of-scope system; attempt to access, alter, or disrupt a third-party or cloud-provider control plane or neighboring tenant except as the written third-party permission and Section 1 expressly allow; persist a backdoor, new account, or implant after the testing window without the Client's written request, and will remove or disclose any temporary access method at the end of the work; or commit a crime, or exceed the authorization granted in this document.

If a method is not listed as authorized in Section 1 and is not clearly required to complete an authorized test, Savisa will treat it as prohibited until the Client authorizes it in writing.

5. Stop and notification procedures

Immediate stop. Savisa will immediately pause or stop testing, and will notify the Client emergency contact, if any of the following occurs: the Client asks Savisa to stop; Savisa reasonably believes a system is becoming unstable, data may be lost, or a person or property may be at risk; Savisa discovers that an asset is out of scope, that authority is missing or withdrawn, or that a third-party term forbids the work; evidence of an active, unrelated security incident or of possible unlawful activity appears, and continuing the test could interfere or cause harm; a legal demand, or a law-enforcement or regulator request, requires a stop; or the testing window ends.

How a stop is requested. The Client may stop the work at any time by telling the Savisa emergency or primary contact, in person, by phone, or by email, using the contacts in Section 3. A verbal stop is effective immediately. The parties will confirm it in writing (including email) as soon as practical.

Notice of significant findings. If Savisa finds a weakness that it reasonably believes is being actively exploited, or that poses an immediate risk of significant harm, Savisa will notify the Client technical or emergency contact promptly, and will not delay that notice until the final report.

Resume. Testing that has been stopped will resume only when the Client's authorized contact has agreed in writing (including email) to resume, and only within the testing window or a written extension.

Incident caused by the test. If Savisa believes the testing itself has caused an unintended outage, data loss, or similar incident, Savisa will stop the related testing, notify the Client emergency contact, and cooperate in recovery as the Client reasonably requests, subject to this Authorization.

6. Data handling, return, and destruction

The Client remains the owner of its data. Savisa will use Client data and test results only to perform this engagement, to prepare the report for the Client, and to meet legal or professional duties that apply.

Collection limit. Savisa will collect and retain the least amount of Client data reasonably needed to perform the work and to document findings. Savisa will not search for, and will not keep, payment-card full data, government identification numbers, or similar sensitive data unless that data is itself the finding and cannot reasonably be described without a limited sample. Any such sample will be minimized, protected, and handled under this section.

Storage. During the engagement, materials will be stored only on agreed systems or encrypted media (to be specified: _____), and will not be stored in an unapproved personal account or unencrypted personal device.

Return or delivery. Savisa will deliver the written report and, at the Client's request, will return Client-owned devices, credentials, and data copies to the Client at the end of the work, using an agreed method: encrypted electronic delivery / in-person return / other, to be confirmed in writing.

Destruction. Unless a law, a legal hold, a dispute, or a written Client request requires or permits a longer period, Savisa will delete or destroy Client data, working notes that contain Client data, and local copies of the report in Savisa's possession within _____ days after the later of (a) delivery of the final report or (b) the end of the testing window, or within a period confirmed in writing before testing begins if no number is named here. Destruction means shredding, erasing, or otherwise modifying the data so they cannot reasonably be read, deciphered, or reconstructed through generally available means. Savisa may retain a copy of this signed Authorization, invoices, and a record that the work occurred, for its ordinary business and legal records.

At the Client's written request, Savisa will confirm in writing that destruction under this section has been completed, except for records this section allows Savisa to keep.

Credentials. The Client will provide only the access needed for the in-scope work, will record what was provided, and may revoke that access at any time. Savisa will not share Client credentials with anyone who does not need them for this engagement, and will return or destroy credential materials at the end of the work.

7. Confidentiality

Each party may receive confidential information of the other, including system details, findings, this Authorization, and non-public business information. The receiving party will use that information only for this engagement, will protect it with reasonable care, and will not disclose it to a third party except: to employees, contractors, or professional advisors who need it for this engagement and are bound to keep it confidential; as the disclosing party has agreed in writing; as required by law, or by a court, regulator, or law-enforcement demand, in which case the receiving party will, if legally permitted, give the other party prompt notice so that it may seek protection; or as needed to report an imminent risk to a person's safety, or to report reasonably suspected unlawful activity to an appropriate authority.

Findings and the report are the Client's confidential information. Savisa will not publish them, and will not identify the Client in marketing, without the Client's prior written consent.

These confidentiality duties continue for _____ years after the end of the testing window (or a period confirmed in writing before testing begins, if none is named here), and indefinitely for trade secrets as long as they remain trade secrets under applicable law.

8. Liability limit and indemnity

Please read this section carefully.

To the fullest extent the law allows, neither party is liable to the other for indirect, incidental, special, consequential, exemplary, or punitive damages, or for lost profits, lost data, or loss of goodwill, arising out of or related to this Authorization or the work, even if told that such damages were possible.

To the fullest extent the law allows, each party's total liability to the other for claims arising out of or related to this Authorization or the work is limited to the fees paid or payable by the Client for this engagement.

These limits do not apply to the extent the law does not allow them. That includes, where the law does not allow a limit, a party's own fraud, willful misconduct, or gross negligence, and any other liability that applicable law says cannot be limited. These limits also do not apply to a party's breach of Section 7 (Confidentiality), to the Client's breach of Section 2 (authority), or to the Client's indemnity below.

Client indemnity. The Client will indemnify, defend, and hold harmless SavIsa Solutions LLC and its members, managers, employees, contractors, and agents from claims, losses, damages, costs, and reasonable attorneys' fees that arise out of or relate to: (a) the Client's lack of authority, or a third party's claim that testing of an asset was not authorized; (b) the Client's breach of this Authorization; or (c) a third-party claim arising from the Client's use of the report, except to the extent caused by Savisa's fraud, willful misconduct, or gross negligence.

This section continues to apply after the testing window ends and after this Authorization otherwise ends.

9. Insurance

The Client should maintain its own insurance for its systems, premises, and business.

10. Governing law

This Authorization is governed by the laws of the State of Michigan, without regard to conflict-of-law rules that would apply another state's law.

11. Electronic signatures; counterparts

The parties agree that this Authorization may be signed in counterparts, including electronic counterparts, and that electronic records and electronic signatures will be used in its formation.

A record or signature will not be denied legal effect or enforceability solely because it is in electronic form. If a law requires a writing or a signature, an electronic record or electronic signature is intended to satisfy that law, as provided by the Michigan Uniform Electronic Transactions Act, MCL 450.831 et seq., including MCL 450.837, and by the federal Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. § 7001.

Each signer represents that they have authority to bind the party in whose name they sign.

Client

Legal name: _____ Signer's name: _____

Title: _____ Signature: _____ Date: _____

Email for notices: _____

SavIsa Solutions LLC, doing business as Savisa Security

Savisa will countersign when the engagement is confirmed. Testing does not begin until Savisa confirms the signed scope.

Signer's name: _____ Title: _____

Signature: _____ Date: _____

Email for notices: _____

By signing, the Client authorizes Savisa to perform the work described in this Authorization, and both parties agree to these rules of engagement.

Savisa Security is a private company and is not affiliated with any government agency.