Security Assessment Agreement

Goal

Parties

This contract agreement (the “Agreement”) is entered into as of by and between (the “Service Provider”), a located at and (the “Recipient”), a located at , (collectively the “Parties”).

Purpose of Agreement

The Recipient requests the Service Provider perform a security assessment (the “Engagement”) by performing work outlined in the attached document titled ”Rules of Engagement”. The Parties therefore agree as follows:

Scope of Work

The Service Provider will provide a security assessment as outlined in the attached document titled ”Rules of Engagement” (”Rules of Engagement”, “Statement of Work”, or “SOW”)

Project Term

This Agreement takes effect immediately as of the Agreement Date, and remains in full force and effect until Service Provider has completed the Engagement (the “Term”), unless earlier terminated by one party under the terms of this Agreement. All Statements of Work will automatically terminate upon early termination of this Agreement.

Changes in Project Scope

If at any time following execution of a Statement of Work by Service Provider, Recipient should desire a change in Service Providers performance under the Statement of Work that will alter or amend the Specifications or other elements of the Statement of Work, Recipient shall submit to Service Provider a written proposal specifying the desired changes.

Acceptance of Deliverables

Recipient must inform Service Provider within business days of receiving any Deliverable of any objections, corrections, changes or amendments Recipient wishes made to such Deliverable. If Recipient does not provide this notice within said stated time period, the Deliverable shall be deemed accepted.

If the Deliverable does not conform to the specifications, Recipient shall give Service Provider written notice stating why the Deliverable is unacceptable. Service Provider shall have days from the receipt of such notice to correct the deficiencies. Recipient shall then have days to inspect, test and evaluate the Deliverable. If the Deliverable still does not conform to the specifications, Recipient shall have the option of either

- repeating the procedure set forth above, or
- terminating this Agreement pursuant to the section of this Agreement entitled “Termination of Agreement or Statements of Work.”

Termination of Agreement or Statements of Work

Either Party may terminate this Agreement at any time, with or without cause, upon written notice.

Either Party also may at any time terminate the Agreement immediately if the other party commits a breach of this Agreement and such party does not cure a breach within of written notice from the non-breaching party of such breach.

Disputes

The parties agree that any and all disputes, claims or controversies arising out of or relating to this Agreement shall be submitted to , or its successor, for final and binding arbitration Judgment on the Award may be entered in any court having jurisdiction. This clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

Force Majeure

Neither Party will not be deemed to be in breach of contract or otherwise responsible for delays or failures in performance resulting from acts of God; acts of war or civil disturbance; epidemics; governmental action or inaction; fires; earthquakes; unavailability of labor, materials, power, or communication; or other causes beyond such Parties reasonable control.

Independant contractor

Service Provider is an independent contractor, and neither Service Provider nor Service Provider's staff is, or shall be deemed, Recipient's employees. In its capacity as an independent contractor, Service Provider agrees and represents, and Recipient agrees, as follows:

1. Service Provider may perform similar services for third Parties using the same personnel that Service Provider may utilize for rendering the Services for Recipient hereunder, subject to Service Provider obligations respecting Recipients's Confidential Information.
2. Service Provider has sole discretion to determine how, when, and where to perform services required to achieve the final result specified in the Scope of Work.
3. The services required by this Agreement shall be performed by Service Provider, or Service Provider's staff, and Recipient shall not be required to hire, supervise or pay any assistants to help Service Provider.
4. As an independent contractor, Service Provider is not eligible for and has no claim to medical benefits, profit sharing, vacation pay, sick pay, or other benefits offered by Recipient to employees.
5. Neither Service Provider nor Service Provider's staff shall be required to devote full-time to the performance of the services required by this Agreement.
6. Recipient shall not provide insurance coverage of any kind for Service Provider or Service Provider's staff.
7. Service Provider, its employees and agents shall be free to use and employ their general skills, know-how, and expertise, and to use, disclose, and employ any generalized ideas, concepts, know-how, methods, techniques or skills gained or learned during the course of any Services performed hereunder, subject to its obligations respecting Recipients's Confidential Information.

General Provisions

1. Complete Agreement: This Agreement together with all exhibits, appendices or other attachments, which are incorporated herein by reference, is the sole and entire Agreement between the parties. This Agreement supersedes all prior understandings, agreements and documentation relating to such subject matter. In the event of a conflict between the provisions of the main body of the Agreement and any attached exhibits, appendices or other materials, the Agreement shall take precedence.
2. Modifications to Agreement: Modifications and amendments to this Agreement, including any exhibit or appendix hereto, shall be enforceable only if they are in writing and are signed by authorized representatives of both Parties.
3. All written notifications must be delivered using unless they contain Confidential Information. If written notifications contain Confidential Information they must follow the guidelines set for communications containing confidential information.
4. Applicable law: This Agreement will be governed by the laws of .
5. No Agency: Nothing contained herein will be construed as creating any agency, partnership, joint venture or other form of joint enterprise between the Parties.
6. Severability: If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement will be interpreted so as best to carry out the parties' intent.
7. Counterparts, Electronic Signatures: This Agreement may be executed in counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instrument. This Agreement may be signed and delivered by facsimile, .pdf format data file or other electronic transmission, and such electronic signatures shall be deemed original signatures for purposes of enforcement and construction of this Agreement.

Signatures

The terms and conditions of this Agreement may be modified or amended as necessary only by written instrument signed by both parties. By signing this Agreement, I indicate that I understand, agree to and accept the terms and conditions listed above and in all referenced documents throughout, dated .

Service Provider

- Name: Anicetas Švedas
- Title: Director
- Date: _____
- Signature: _____

Recipient

- Name: Zou Woei-wan
- Title: CEO
- Date: _____
- Signature: _____

Rules of Engagement

Representations and Warranties

For the purpose of this Agreement, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:

- Service Provider will make every effort to avoid disrupting Recipient's work environment more than is reasonable to conduct an assessment.
- Recipient understands that Service Provider is not an employee, and that this will be a collaborative, professional relationship of equals where mutual professional respect, courtesy and consideration are expected.
- Recipient's personnel will provide the Security Providers with all information requested to complete this engagement in a timely manner.
- Recipient agrees that the accuracy of information supplied to Service Provider is the sole responsibility of Recipient, and that Service Provider is not responsible and shall not be held liable for the results of services performed on the basis of inaccurate, incomplete or untruthful information furnished by Recipient.
- The recipiant is authorized to give authorization to the Service Provider to perform these activities on all systems, networks, and devices.
- The recipiant has informed the Service Provider of all systems on the network, or included within the testing scope, which the client does not own, and that may require additional approval to test.
- Recipient will provide full access to all Recipient participants and personnel, as required, throughout the duration of the engagement.
- Recipient will provide Service Provider adequate workspace and Internet connections while on site to access email and other online resources.
- Recipient understands that Service Provider is a business with other clients to serve, and requires fair, realistic notice in order to attend to requests and projects.
- Consultant warrants and represents that it shall not knowingly, or with negligence, include or authorize any Trojan Horse, back door, time bomb, drop dead device, worm, virus, or other malicious code of any kind that may disable, erase, display any unauthorized message or otherwise impair the Company's software, with disregard of the possibility of or the intent to cause harm.
- The Service Providers performance of the Services called for by this Agreement does not and shall not violate any applicable law, rule, or regulation or any contracts with third parties.
- The materials to be prepared, produced or developed for Company do not and shall not violate any third-party rights in any patent, trademark, copyright, trade secret, or similar right.
- Servcie Provider is the lawful owner or licensee of any software programs or other materials not provided by Company but used by Service Provider in the performance of the Services called for in this Agreement.
- Service Provider has all rights necessary to convey to Company the unencumbered ownership of the materials developed by Spohn under this Agreement.
- Consultant will cause its personnel to comply with all of Company's lawful standards and procedures when working on-site at Company's facilities, including standards and procedures relating to security, provided that Consultant is given advanced notice of such standards and procedures.
- Service Provider has the experience and ability to do everything agreed to for Recipient and will do it all in a professional and timely manner.

- Service Provider is independent, non-product affiliated, and not in the business of selling security systems hardware.
- Service Provider will provide documentation on the setup and use of the tools required for being an emergency contact before the start of the Engagement.
- Service provider will provide training to point of contact on tools required for secure handling of confidential information [BEFORE/DURING] [PHASE OF ENGAGEMENT].
- Service Provider will make themselves available before and during the Engagement to provide additional guidance as needed to allow them to safely carry out their role.

Scope of Work

The Assessment component of the Engagement will consist of the following phases:

Assessment preparation

- **Begins:** after the signing of the agreement
- **Duration:** one month
- **Total Time:** two weeks
  To commence our engagement Service Provider will meet with IT/Operations leadership for an initial description of the situation and current landscape. Following that session Recipiant will provide Service Provider with any research materials that will be useful to inform Service Provider's knowledge of the organization its infrastructure work and the risks it faces.

Reconnaissance

- **Begins:** alongside assessment preparation
- **Duration:** the entire length of the assessment
- **Total Time:** 15 days
  The Service Provider will identify publicly available resources (such as websites, extranets, email servers, but also social media information) connected to the organization and remotely gather information about those resources. It will include both passive reconnaissance of publicly available data sources and active external scans of Recipients network assets.

Data assessment

- **Begins:** at the start of the on-site engagement phase
- **Duration:** throughout the length of the on-site phase
- **Total Time:** 3 days
  Service Provider will lead staff in activities where they identify where critical data currently resides (what devices/physical locations), who has access (physical, login, permissions), and who needs to have access to do their jobs.

Threat assessment

- **Begins:** for two days
- **Duration:** on the first day of the on-site engagement
- **Total Time:** 8 days
  The Service Provider will carry out a variety of activities to identify possible attackers and gather background information about the capability of those attackers to threaten the Recipients organization. This will include identifying a particular attacker's history of carrying out specific threats, their capability to carry out those threats currently, and intent to expend their resources against the Recipient.

Report Writing

- **Begins:** after all on-site activities have completed
- **Duration:** 30 days
- **Total Time:** 10 days
  The Service Provider will compile their assessment notes and recommendations into a comprehensive set of documents the shows the current state of security, the process by which the Service Provider came to that assessment, and recommendations that will guide Recipient's progression to meet their security goals.

Feedback and follow up activities

- **Begins:** upon acceptance of final report
- **Duration:** up to 30 days
- **Total Time:** up to 5 days
  The Service Provider will lead a meeting with the primary point of contact to deliver and discuss the reports findings as well as a final follow-up meeting to explain recommendations and answer staff questions.

Estimated Engagement Schedule

Activity	Estimated Start Date	Estimated Duration
Assessment preparation	after the signing of the agreement	one month
Reconnaissance	alongside assessment preparation	the entire length of the assessment
Data assessment	at the start of the on-site engagement phase	throughout the length of the on-site phase
Threat assessment	for two days	on the first day of the on-site engagement
Report Writing	after all on-site activities have completed	30 days
Feedback and follow up activities	upon acceptance of final report	up to 30 days

Incident Response Procedures

If either Party identifies a suspected or known security incident during the Engagement (such as previous or active compromise to the Recipient's systems) they will suspend any assessment activities and inform the emergency contact(s) provided by the other party using one of the approved methods for secure communication within . Information security incidents include a suspected, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of information; interference with information technology operations; or interference with system operations.

The extent to which assessment activities will be suspended, and the degree to which incidents must be addressed for activities to continue will be decided per-incident based upon an agreement by both parties.

The extent to which assessment activities should be suspended will vary based on the the type of incident, but in many cases the only activities suspended are those involving the systems directly involved in the incident.

Emergency Contacts

The Parties ability to be able to get in touch in an emergency is vital. Emergencies may arise, and each Party must have an established point of contact in order to handle them. Each Party will designate one or more emergency contacts. Each party will give a list containing the following information about each of those contacts to the other party.

- Full name:
- Title and operational responsibility:
- One to two forms of 24/7 immediate contact: (such as cell phone, pager, or home phone)
- One form of secure bulk data transfer: (such as SFTP or encrypted email)

Recipient Contacts

Full Name	Immediete Contact	Immediete Contact	Secure Data Transfer
Maral Mansur	Cell Phone: +1-555-524-9078	Home Phone: +1-555-254-0971	OnionShare
Zou Woei-wan	Cell Phone: +1-555-884-1412	Home Phone: +1-555-884-5793	Peerio

Service Provider Contacts

Full Name	Immediete Contact	Immediete Contact	Secure Data Transfer
Chun Sang-jin	Cell Phone: +1-555-264-0798	Home Phone: +1-555-245-7091	OnionShare
Martínez Buentello	Cell Phone: +1-555-657-0228	Signal (iPod): +1-555-675-2082	Peerio

Service Provider Role in Addressing Incidents

When a security incident has been identified the Parties will come to an agreement as to whether the incident should be addressed immediately, or should be addressed after the Engagement.

Confidential Information

During the term of this Agreement and for years afterward, each party will use reasonable care to prevent the unauthorized use or dissemination of the other party's Confidential Information. Reasonable care means that each party treats the other party's data with at least the same degree of care that a party uses to protect its own confidential information from unauthorized disclosure.

Confidential Information is limited to:

- information about the Recipants's business or computer systems or security situation that Service Provider obtains during the course of it's work (including, but not limited to all security findings, results, and recommendations); and
- information clearly marked as confidential, or disclosed orally that is treated as confidential when disclosed and summarized and identified as confidential in a writing delivered to the receiving party within days of disclosure.

Confidential information does not include information that:

- the receiving party knew before the disclosing party disclosed it
- is or becomes public knowledge through no fault of the receiving party

- the receiving party obtains from sources other than the disclosing party who owe no duty of confidentiality to the disclosing party, or
- is independently developed by the receiving party.

Where disclosure to a third party is essential, the party wishing to disclose the information shall obtain prior written authorization to do so from the other party.

Judicial Requests or Other Government Orders

In the event either party is required to disclose Confidential Information pursuant to a judicial or other governmental order, such party shall, to the maximum extent permitted by law or opinion of counsel, provide the other party with prompt notice prior to any disclosure so that the party may seek other legal remedies to maintain the confidentiality of such Confidential Information.

Information Security Safeguards

Device Security

Service Provider will secure all the devices they will use for the assessment. This includes

- All devices will have full-disk encryption enabled and will be powered down when traveling.
- All mobile devices will have remote wipe enabled
- All passwords used on devices will meet or exceed complex password standards
- All passwords pertaining to the Recipiants assessment - including, but not limited to Wi-Fi, device, and service passwords - will be stored in a password manager under an assessment specific keering and treated as confidential information
- All devices will be fully wiped and/or “factory reset” upon the completion of the assessment

Communications Security

It will often be essential that confidential information be shared between the Recipient and Service Provider. In these situations, the Parties will adhere to the following standards:

Data Storage and Destruction

The Service Provider will create and collect a range of confidential information during the assessment. The Service Provider will adhere to the following standards in regards to the storage and destruction of data and documents containing confidential information:

- When destroying confidential material Service Provider will permanently delete all electronic data from all Service Provider’ devices and hardcopy documents containing confidential information will be destroyed by shredding, tearing in small pieces, or burning.
- Service Provider will destroy all confidential material they still have in their possession after the Engagement.

The Recipient will is likely to be provided sensitive information as a part of this assessment. The Recipient will adhere to the following standards in regards to the storage and destruction of data and documents containing confidential information:

Authorized Recipients Of Confidential Information

The above “Privacy and Security” and “Safeguards to Protect Confidential Data and Communications” statements define the entire agreement between the involved parties concerning the circulation and disclosure of Confidential Information.

The receiving parties agree not to disclose such information to any party not defined in this document as an ”authorized” party.

By signing below, the authorized parties signify that they understand and agree to the terms of this legally binding document.

Authorized Recipients Of Confidential Information

Party	Full Name	Signature
Recipiant	Zou Woei-wan	
Recipiant	Maral Mansur	
Recipiant	Zou Woei-wan	
Service Provider	Chun Sang-jin	
Service Provider	Martínez Buentello	

Signatures

By signing this document, gives permission to conduct the above Statement of Work and agrees to adhere to the terms and conditions aforementioned in this document.

By signing this document, agrees to conduct to the above Statement of Work. also agrees to adhere to the terms and conditions aforementioned in this document.

Anicetas Švedas

Zou Woei-wan