Security Assessment Agreement

Goal

Parties

This contract agreement (the "Agreement") is entered into as of by and between (the "Service Provider") and (the "Recipient"), (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"

Changes in the Scope

The current timeline is based on the scope of work, deliverables outlined, and availability of the Service Provider. In the event that the scope of work changes, service provider will provide you with a statement that includes the updated Scope of Work and any impact the proposed changes will have on the delivery dates of the SOW. Your signature on such document will be considered an amendment to this letter of agreement.

Term and Termination

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 SOWs will automatically terminate upon early termination of this Agreement.

How can we terminate this agreement?

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.

What happens if we terminate this agreement?

Termination for any reason shall not affect the either Parties rights and/or responsibilities as outlined in the Privacy and Security section.

Are there any exceptions?

Neither Party will not be deemed to be in breach of contract or otherwise responsible for delays or failures in performance resulting from **security incidents identified during the Engagement;** 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 that Parties reasonable control.

Disputes

Disputes will be settled through binding arbitration

Any dispute, claim or controversy arising out of or relating to this Agreement before one arbitrator. Judgment on the Award may be entered in any court having jurisdiction. The parties will share the costs of the arbitrator equally. This clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

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 .

Zou Woei-wan:

_____

Anicetas Švedas:

_____

Rules of Engagement

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.

Assumptions and Limitations

- 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 will endeavor to meet every deadline and perform the Engagement in accordance with the sector's best practices.
- Service Provider will make every effort to avoid disrupting the Recipient's work environment more than is reasonable to conduct an assessment.
- The Recipient's personnel will provide service providers with all information requested to complete this engagement in a timely manner.

- The Recipient will provide full access to all Recipient participants and personnel, as required, throughout the duration of the engagement.
- The Recipient will provide Service Provider adequate workspace and Internet connections while on site to access email and other online resources.
- If the Recipient's emergency contacts do not have experience using the communication security practices outlined above Service Provider will guide them through the setup and use of the tools required.
- Service Provider is independent, non-product affiliated, and not in the business of selling security systems hardware.

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 .

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.

Privacy and Security

- All Engagement findings, results, and recommendations are confidential and will be treated as such.
- Service Provider will not share any information that has been disclosed between Parties in relation to the Engagement.
- Confidential information will only be used for the purpose of the Engagement.
- 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.

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 via prior to any disclosure so that the party or its client may seek other legal remedies to maintain the confidentiality of such Confidential Information.

Safeguards to Protect Confidential Data and Communications

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