Security Assessment Agreement

Goal

The traditional corporate security assessment is based upon an assumption that an organization has the time, money, and manpower to aim for as close to perfect security as possible, and more importantly, that they will be able to have ongoing assessments over time. The Recipient of this assessment has none of these luxuries.

Therefore they have asked the Service Provider to design and use a customized combination of selected assessment techniques derived from standards in the security auditing world to provide a tailored risk assessment and mitigation consultation.

This audit will not only provide an assessment of the Recipients risks, but will also act as a teaching opportunity for the Service Provider to provide the Recipient a map of their digital footprint, an understanding of how their technology is tied to the threats they perceive, and guidance on how to seek out support in the future.

Lastly, the Service Provider is well connected to trusted digital security trainers around the world as well as large networks of resources and broader capabilities, including rapid response networks. They will use these preexisting relationships to help the Recipient identify the support they need to address their vulnerabilities.

Parties

This contract agreement (the "Agreement") is entered into as of July 12th, 2016 by and between ABC Assessing (the "Service Provider") and XYC Company (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 30 days 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 15 days 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 mediation and the costs will be shared

If a dispute arises, the parties will try in good faith to settle it through a mediator to be mutually selected.

The parties will share the costs of the mediator equally. Each party will cooperate fully and fairly with the mediator and will attempt to reach a mutually satisfactory compromise to the dispute.

If not resolved in mediation it will be submitted to binding arbitration

If the dispute is not resolved within 30 days after it is referred to the mediator, it will be settled by binding arbitration in Washington, DC or another location mutually agreeable to the parties. The parties will share the costs of the arbitrator equally. An award of arbitration may be confirmed in a court of competent jurisdiction.

If arbitration or litigation is required the party who loses pays the other party's attorney's fees

In the event of arbitration, or litigation relating to the subject matter of this Agreement, the prevailing party shall have the right to collect from the other party its reasonable costs and necessary disbursements and attorneys' fees incurred in enforcing this Agreement.

Indemnification and Liability

The Recipient understands that digital security is a continually growing and changing field and that security guidance provided by Service Provider does not mean that the Recipient will be able to secure their software from every form of attack. There is no such thing as 100% security, and for example it is never possible to identify vulnerabilities in software or systems for threats that are not known at the time of the assessment.

Who is responsible if recipiant suffer a breach or other cyber-security incident in the future?

Recipiant assumes sole and total responsibility and risk for any damages or liabilities arising directly or indirectly out of the services, this agreement, service provider's performance of this agreement, any obligations resulting therefrom, and Recipiants's reliance thereon; and recipiant agrees that any such damages or liabilities are not the responsibility of service provider.

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 July 12th, 2016.

Anicetas Švedas:

_____

Soraya Herce:

_____

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
  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
  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
  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
  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
  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 approval of final report
- **Duration:** up to 15 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.

Update Meetings

- **Begins:** Start of Assessment
- **Duration:** Full Length of Assessment
  Additionally, service providers designated contact (Maral Mansur) will hold meetings with recipiants designated contact (Zou Woei-wan), once a week, to inform them of the overall progress of the assessment.

Deliverables

What deliverables will be produced during the Engagement?

Service Provider will provide the following deliverables to the Recipient.

- A report that shows the Recipient's current state of security, the process by which the Service Provider came to these conclusions, and recommendations that will guide the Recipient's progression to meet their security goals.

Who will the report be written for?

Service Provider will tailor the report for its targeted audiences in the following ways:

- The report will contain an easy-to-read executive summary with no technical jargon.
- The report will contain sufficient detail that later technical and/or security teams will be able to implement the recommendations.
- Each recommendation will include a summary statement that shows proof of need and contains no sensitive information. These statements will be written in a way that will allow the Recipiant to directly copy them into funding proposals.

What do I do if the deliverables are not complete or if I want changes made?

The Recipient must inform Service Provider within 15 business days of receiving any Deliverable of any objections, corrections, changes or amendments Client wishes made to such Deliverable. If the Recipient does not provide this notice within said stated time period, the Deliverable shall be deemed accepted.

How many revisions can I request?

The Recipient can request up to 1 revisions to a deliverable.

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 1 business day.

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	Phone Number	Secure Channel
Gianetta Morbidelli	+353 20 913 XXXX	pgp: gmorbidel@example.com
Miguel Martínez Buentello	+353 20 139 XXXX	pgp: mmb2017@example.com
Zou Woei-wan	+353 05 913 XXXX	Signal: Same Number

Service Provider Contacts

Full Name	Phone Number	Secure Channel
Maral Mansur	+36 55 754 XXX	Signal: Same Number
Chun Sang-jin	+36 55 774 XXX	PGP: ItsAMeSangJin@example.com

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.

If the Parties decide that the security incident should be addressed immediately Service Provider will mitigate, to the extent practicable, the harmful effects of the security incident that are known to Service Provider; and document security incidents and their outcomes.

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.
- Both Parties will keep this Agreement confidential, and will not disclose either the existence or the terms of the Agreement to third parties.
- 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.

Exceptions

Service Provider is able to provide the following information to the third-party funder of the Engagement (the "Funder").

- the number of vulnerabilities identified
- the specific vulnerabilities that are identified

All information provided to the Funder will comply with the same Communications Security practices described in the next section.

Service Provider will take the following additional actions to reduce any risk to the Recipient when sharing this information.

- the Recipient's location, name, and type of work will not be disclosed
- the Recipients vulnerabilities will be aggregated with the vulnerabilities of two or more other Recipients the Service Provider is funded to assess.

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 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:

- Any confidential information shared between the Parties via email must be encrypted.
- Any deliverables containing confidential information must be encrypted and password-protected.
- All passwords used for deliverables will meet or exceed complex password standards.
- Any passwords that need to be communicated will be communicated in person or via an encrypted voice and/or video platform.

Data Destruction

At the conclusion of the on-site portions of the Engagement, all engagement workpapers and hardcopy documents will be digitized, encrypted and stored on a secure file server by Service Provider. Service Provider will destroy the above hardcopy documents using the destruction practices described below.

Service Provider will destroy all confidential material One Year after the Engagement.

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.

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.

The third parties identified in the Exceptions subsection to the Privacy and Security section are considered “authorized” parties for the specific pieces of information outlined in that section

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	Gianetta Morbidelli	
Recipiant	Miguel Martínez Buentello	
Recipiant	Zou Woei-wan	
Service Provider	Maral Mansur	
Service Provider	Chun Sang-jin	

Signatures

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

Anicetas Švedas:

Soraya Herce: