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 estimate outlined in the Section Payment Schedule of the Rules of Engagement is based on the scope of work and deliverables outlined. In the event that the scope of work changes, service provider will provide you with either a change order to this estimate or a new estimate covering the new project deliverables or added scope. Your signature on such document will be considered an amendment to this letter of agreement.

Subcontracting

Service Provider shall not subcontract its obligations under this Agreement to another person or entity, in whole or in part, without Recipients prior written approval.

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 15 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 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, either party may submit it for 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. This clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate 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.

Limitations on Liability

Recipient understands that digital security is a continually growing and changing field and that security guidance provided by Service Provider does not mean that Recipient will be able to secure their software and systems 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.

Recipient 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 Recipients's reliance thereon; and Recipient agrees that any such damages or liabilities are not the responsibility of Service Provider.

Without limiting the foregoing, Service Provider and its officers, directors, employees and agents will in no event be liable for any special, incidental, consequential, or any other indirect loss or damage of any nature, including without limitation lost profits or lost revenues, caused to the business or property of Recipient or anyone else arising out of or related to the services, this agreement, Service Providers's performance of this agreement, any obligations resulting therefrom, and Recipients's reliance thereon.

The entire, aggregate, and maximum liability, if any, of Service Provider, its officers, directors, employees and agents for any and all claims, losses, damages, or expenses arising out of or related to the services, this agreement, Service Provider's performance of this agreement, any obligation resulting therefrom, and Recipients's reliance thereon, shall in no event be greater than the amount paid by Recipient to Service Provider under this agreement.

This limitation of liability is an essential and bargained for part of this agreement, and Service Provider would not perform the services without this limitation. No representative of Service Provider has authority to verbally modify the terms of this limitation.

Indemnification

Each party will indemnify the other party from any third-party claims resulting in losses, damages, liabilities, costs, charges, and expenses, including reasonable attorney fees, arising out of any breach of the indemnifying party's representations and warranties contained in this Agreement, or, in the case of Client's indemnification of Contractor, arising out of the use of Services provided under this Agreement.

Ownership of Work Product

Service Provider shall retain all copyright, patent, trade secret and other intellectual property rights Service Provider may have in anything created or developed by Service Provider for Recipient under this Agreement and any Statement of Work.

Survival

The provisions of the Sections "Disputes", "Attorney Fees", "Ownership of Work Product", and "Limited Liability" within this Agreement and the Sections "Confidential Information" and "Information Security Safeguards" within the Rules of Engagement will survive any termination of this Agreement.

Payment

Payment Terms

The Recipient understands the importance of paying Service Provider in a timely manner and wants to maintain a positive working relationship with Service Provider to keep the project moving forward.

Payments for each invoice delivered by Service Provider to the Recipient are due within 30 days of receipt. In case of overdue payments, Service Provider reserves the right to stop work until payment is received.

Late Payment

In the event an invoice is not paid on time, to the maximum extent allowable by law, Service Provider will charge a late payment fee of 1.5 per 30 days on any overdue and unpaid balance not in dispute.

Expense Reimbursement

The Recipient shall reimburse all expenses that are reasonable and that have been authorized in writing by the Recipient in advance; payable within 30 days of itemized invoice. Payments should be wired directly into Service Providers account. Service Provider will provide account details on the invoice.

Recipiant shall reimburse service provider for all reasonable out-of-pocket expenses incurred by service provider in performing services under this Agreement as long as such expenses are approved by recipiant in advance. Such expenses include, but are not limited to:

1. third-party expenses for online services, such as hosting and/or computing;
2. Service Provider travel required in the performance of the Engagement; and
3. other expenses resulting from the work performed under 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 July 12th 2016.

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.

Update Meetings

- **Begins:** Status updates will start when Assessment activities begin
- **Duration:** Status updates will end when reporting begins
  Additionally, service providers designated contact False will hold meetings with the Recipient's point of contact, every 15 days to inform them of the overall progress of the assessment.

Activities Not Included

In general, it should be ensured that actual operations in the organisation are not significantly disrupted by the assessment during the Engagment. The Service Provider will never actively intervene in systems, and therefore will not provide any instructions for making changes to the systems being audited.

Payment Schedule

Payments will be made to Service Provider for completion of milestones in accordance with the following payment schedule.

Milestone	Estimated Completion Date	Payment Due on Delivery
Remote Assessment	2016-09-30	20000
On-Site Assessment	2016-10-30	20000
Reporting	2016-11-15	20000
Follow Up	2016-12-01	20000
Total		80000

Deliverables

What deliverables will be produced during the Engagement?

Service Provider will provide the following deliverables to the Recipient.

Assessment Report

Due: Nov 25th, 2016
This report 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.

Info-Sec Training Curricula

Due: Jan 4th, 2017
Increase the quality and capability of the Recipiants in-house information security program.

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

The Recipient must inform Service Provider via email 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 3 revisions to a deliverable.

Beyond the included 3 round(s) of revisions will be billed at the following rates.

Service	Description	Hourly Rate	Minimum Hours
Illustration Creation	The creation of explanatory and/or educational illustrations	50	3
Content Updates/Additions	Updates and/or additions to text based content in a report.	100	2

What if the Service Provider needs to extend the delivery date?

Service Provider will use all reasonable efforts to deliver the Deliverables on schedule. However, at its option, Service Provider can extend the due date for any Deliverable and/or Milestone by giving written notice to Recipient. This notice must be provided to Recipient 15 days before the Deliverable due date. The total of all such extensions shall not exceed True days.

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 2 days.

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.

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.

Incidents Triggered by Assessment Activities

The Service Provider commits to prioritizing the stability and integrity of the Recipiant's digital infrastructure over any additional testing could be carried through more aggressive methods.

No tests will be performed that would stress the network, or any individual workstation, beyond what could be expected from normal use. If Service Provider has any doubt, Service Provider will consult with Recipient before carrying out the test.

In the unlikely event that Service Provider causes network or system disruption/damage, any active procedures will be terminated. Service Provider will then follow the security incident procedures described above.

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

Exceptions

Service Provider is able to provide the number of incidents identified and their types. (the "Third Party")to my best friend.

All information provided to the Third Party 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.

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 email 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.
- 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 they still have in their possession 180 days 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.

The third parties identified in the Exceptions subsection to the Privacy and Security section are considered "authorized" parties for the speicfic 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	Zou Woei-wan	_____
Recipiant	Maral Mansur	_____
Recipiant	Zou Woei-wan	_____
Service Provider	Chun Sang-jin	_____
Service Provider	Martínez Buentello	_____

Signatures

By signing this document, XYC Company gives ABC Assessing 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, ABC Assessing agrees to conduct to the above Statement of Work. ABC Assessing

also agrees to adhere to the terms and conditions aforementioned in this document.

Anicetas Švedas

_____

Zou Woei-wan

_____