

# 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"), a Washington, DC Corporation located at 1600 Pennsylvania Ave NW, Washington, DC 20500 and XYZ Company (the "Recipient"), a Colorado 501(c)(3) nonprofit corporation located at 1600 Pennsylvania Ave NW, Washington, DC 20500, (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") which is estimated to be December 1st, 2016, 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.

Service Provider will evaluate each such proposal at its standard rates and charges. Service Provider shall submit to Recipient a written response to each such proposal within 15 working days following receipt thereof. Service Providers written response shall include a statement of the availability of Service Providers personnel and resources, as well as any impact the proposed changes will have on the contract price or delivery dates of the SOW, or the warranty provisions of this Agreement. The signature of Recipient's authorized representative on such a document will be deemed to be approval of the modification and any associated fees.

## **Acceptance of Deliverables**

Recipient must inform Service Provider within 15 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 15 days from the receipt of such notice to correct the deficiencies. Recipient shall then have 15 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."

Revisions to deliverables made to correct deficiencies do not count towards the 1 revisions Recipient is allowed as outlined in the Section "Deliverables" within the Rules of Engagement.

## **Additional Work and Addressing Vulnerabilities**

The parties shall collaborate in good faith on all future work, if any, beyond the Initial Statement of Work, including for Assessment related incident response, security guidance, and vulnerability mitigation. The Rules of Engagement sets forth a Rate Schedule for such activities, which may change from time to time during the Term of the Engagement on at least 15 days' notice to Recipient. After the Term of the Engagement Service Providers rates are subject to change without notice at the discretion of Service Provider.

## **Termination of Agreement or Statements of Work**

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.

## **Disputes**

The parties agree that any and all disputes, claims or controversies arising out of or relating to this Agreement shall be submitted to JAMS, or its successor, for mediation, and if the matter is not resolved through mediation, then it shall be submitted to JAMS, or its successor, for final and binding arbitration pursuant to the clause set forth in Paragraph 5 below.

1. Either party may commence mediation by providing to JAMS and the other party a written request for mediation, setting forth the subject of the dispute and the relief requested.
2. The parties will cooperate with JAMS and with one another in selecting a mediator from the JAMS panel of neutrals and in scheduling the mediation proceedings. The parties agree that they will participate in the mediation in good faith and that they will share equally in its costs.

3. All offers, promises, conduct and statements, whether oral or written, made in the course of the mediation by any of the parties, their agents, employees, experts and attorneys, and by the mediator or any JAMS employees, are confidential, privileged and inadmissible for any purpose, including impeachment, in any arbitration or other proceeding involving the parties, provided that evidence that is otherwise admissible or discoverable shall not be rendered inadmissible or nondiscoverable as a result of its use in the mediation.
4. Either party may initiate arbitration with respect to the matters submitted to mediation by filing a written demand for arbitration at any time following the initial mediation session or at any time following 45 days from the date of filing the written request for mediation, whichever occurs first ("Earliest Initiation Date"). The mediation may continue after the commencement of arbitration if the parties so desire.
5. At no time prior to the Earliest Initiation Date shall either side initiate an arbitration or litigation related to this Agreement except to pursue a provisional remedy that is authorized by law or by JAMS Rules or by agreement of the parties. However, this limitation is inapplicable to a party if the other party refuses to comply with the requirements of Paragraph 3 above.
6. All applicable statutes of limitation and defenses based upon the passage of time shall be tolled until 30 days after the Earliest Initiation Date. The parties will take such action, if any, required to effectuate such tolling

## **Attorney 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.

## **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 **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 beyond such Parties reasonable control.

## **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.

## **Limited 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.

## **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, Service Provider's staff or subcontractors, 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. Recipient shall not withhold from Service Provider's compensation any amount that would normally be withheld from an employee's pay.
8. 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. Applicable law: This Agreement will be governed by the laws of Washington, DC.
4. No Agency: Nothing contained herein will be construed as creating any agency, partnership, joint venture or other form of joint enterprise between the Parties.
5. Assignment: The rights and obligations under this Agreement are freely assignable by either party. Recipient shall retain the obligation to pay if the assignee fails to pay as required by this Agreement.
6. Successors and Assigns: This agreement binds and benefits the heirs, successors and assigns of the parties.
7. 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.
8. 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 July 12th, 2016.

### Service Provider

- Name: Soraya Herce
- Title: Principal Consultant
- Date: \_\_\_\_\_
- Signature: \_\_\_\_\_

### Recipient

- Name: Anicetas Švedas
- Title: CEO
- Date: \_\_\_\_\_
- Signature: \_\_\_\_\_

## Rules of Engagement

### Service Provider Representations and Warranties

- 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 understands that Recipient is taking part in this Engagement in support of their work. Service Provider will make every effort to avoid disrupting Recipient's work environment more than is reasonable to conduct an assessment.

- Service Provider is independent, non-product affiliated, and not in the business of selling security systems hardware.
- Because of the nature of the Engagement Service Provider understands that one or more of Recipient's emergency contacts may not have experience using the communication security practices required to support the Engagement. Service Provider will provide documentation on the setup and use of the tools required before the start of the Engagement. Service Provider will also make themselves available before and during the Engagement to provide additional guidance as needed to allow them to safely carry out their role.

## **Recipient Representations and Warranties**

### **Scope of Work**

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

#### **Assessment preparation**

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 Recipient 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**

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 Recipient's network assets.

#### **Data assessment**

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**

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 Recipient's 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**

The Service Provider will compile their assessment notes and recommendations into a comprehensive set of documents that 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**

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

Additionally, the Maral Mansur will hold meetings with the Zou Woei-wan, once a week, to inform them of the overall progress of the assessment.

## Rate Schedule

Agreed upon work beyond the initial “Scope of Work” will be billed at the following rates.

Activity	Comments	Hourly Rate
Consulting – Principal	Consulting on strategy and security architecture specification.	500
Consulting - Policy/Practice	Consulting on security policy and practice development.	500
System Configuration	Configure networks, systems, and software to respond to identified vulnerabilities	500
Training	Provide security training’s on identified topics	500
Development	Writing security budgets and grant and proposal language.	500

## Deliverables

Service Provider will provide the following deliverables to 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.

The report will contain 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.

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 Recipient to directly copy them into funding proposals.

Recipient can request up to 1 revisions to a deliverable.

## 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

Activity	Estimated Start Date	Estimated Duration
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 approval of final report	up to 15 days

## Incident Response Procedures

If either Party identifies an information security incident (“Information Security Incident”) during the Engagement 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. 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	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.

## **External Notification and Communication**

Service Provider agrees that it shall not inform any third party of any Information Security Incident without first obtaining Recipient's prior written consent, other than to inform a complainant that the matter has been forwarded to Recipient. Further, Service Provider agrees that Recipient shall have the sole right to determine: (i) whether notice of the Information Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Recipient's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

## **Confidential Information**

During the term of this Agreement and for 5 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 Recipients'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);
- information about this contract, contract terms, or contract fees; 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 15 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.

## **Funder Information Sharing**

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

The Funder has agreed to comply with the Communications Security practices outlined in the “Information Security Safeguards” Section when receiving the above information.

Service Provider will take the following additional actions to reduce any risk to 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.

## **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 Recipients assessment - including, but not limited to Wi-Fi, device“, and service passwords - will be stored in a password manager under an assessment specific “keyring” 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 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, and/or burning.

### Authorized Recipients Of Confidential Information

The above “Confidential Information” and “Information Security Safeguards” 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 “Funder Information Sharing” subsection to the “Confidential Information” 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
Recipient	Gianetta Morbidelli	_____
Recipient	Miguel Martínez Buentello	_____
Recipient	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:

\_\_\_\_\_