Security Assessment

Goal

{{BEFORE WRITING YOUR AGREEMENT, DECIDE WHAT YOUR GOALS ARE FOR THE CONTRACT. EVERY ASSESSMENT SHOULD BE GOAL-ORIENTED. INSERT WHAT YOUR GOAL IS HERE. A GOOD LEGAL CONTRACT IS ONE THAT CAPTURES THE INTENTIONS OF THE PARTIES ACCURATELY.}}

Parties

This contract agreement (the "Agreement") is entered into as of {{DATE CONTRACT TAKES FORCE}} by and between {{ASSESSOR NAME}} (the "Assessor") and {{RECIPIENT NAME}} (the "Recipient") of the security assessment, (collectively the "Parties").

Assessor

- Name: {{ASSESSOR REPRESENTATIVE NAME}}
- Title: {{ASSESSOR REPRESENTATIVE TITLE}}
- Date: _____
- Signature: _____

Recipient

- Name: {{RECIPIENT REPRESENTATIVE NAME}}
- Title: {{RECIPIENT REPRESENTATIVE TITLE}}
- Date: _____
- Signature: _____

The Recipient requests the Assessor perform a security assessment, (the "Engagement") and may request the Assessor perform other services in the future; and

The Parties therefore agree as follows:

Term and Termination

This Agreement takes effect immediately as of the Agreement Date, and remains in full force and effect until the Assessor has completed the Engagement (the "Term"), unless earlier terminated under the following conditions.

How can we terminate this agreement?

Either Party may terminate this Agreement at any time, with or without cause, upon {{PERIOD OF NOTICE NEEDED FOR TERMINATION}} 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 {{PERIOD FOR BREACH TO BE REMEDIED}} of written notice from the non-breaching party of such breach.

What happens if we terminate this agreement?

If this Agreement is terminated earlier by Recipient without cause, Recipient agrees to pay Assessor any and all sums which are due and payable for:

- services provided as of the date of termination; and
- expenses already incurred, including those from documented non-cancelable commitments. Assessor agrees to use the best efforts to minimize such costs and expenses.

Upon termination, Recipient shall pay to Assessor all undisputed amounts due and payable. If upon termination Recipient has not paid undisputed fees owed for the material, deliverables or Services provided by Assessor as of the date of termination, Recipient agrees not to use any such material or the product of such Service, until Recipient has paid Assessor in full.

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.

Scope of Work

The Assessor will provide a security assessment as outlined in the attached document titled "Rules of Engagement"

Deliverables

What deliverables will be produced during the Engagement?

The Assessor will provide the following deliverables to the Recipient.

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

Who will the report be written for?

The Assessor will tailor the report for its targeted audiences in the following ways:

- {{A way the report is tailored.}}
- {{i.e. The report will contain an easy-to-read executive summary with no technical jargon.}}
- {{i.e. The report will contain sufficient detail that later technical and/or security teams will be able to implement the recommendations.}}
- {{ i.e. 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.}}
- {{ i.e. 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 the Assessor within {{NUMBER OF BUSINESS DAYS}} 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 {{NUMBER OF REVISIONS}} revisions to a deliverable.

Beyond the included {{NUMBER OF REVISIONS}} round(s) of revisions per document will be billed at {{ASSESSORS DAILY/HOURLY RATE}} with a minimum duration of of work.

Indemnification and Liability

Is the Assessor responsible if we suffer an attack in the future?

The Recipient understands that digital security is a continually growing and changing field and that security guidance provided by the Assessor 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.

The Assessor shall be under no liability whatever to the Recipient for any indirect loss and/or expense (including loss of profit) suffered by the Recipient arising out of their security.

Payment

Payment Terms

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

Payments for each invoice delivered by the Assessor to the Recipient are due within {{DAYS UNTIL PAYMENT DUE}} days of receipt. In case of overdue payments, the Assessor 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, the Assessor will charge a late payment fee of {{LATE FEE PERCENT-

AGE}}% per {{PERIOD UNTIL DUE}} 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 {{DAYS UNTIL PAYMENT DUE}} days of itemized invoice. {{EXPENSE REIMBURSEMENT CONDITIONS}}

Any Assessor travel required in the performance of the engagement will be paid for by {{RESPONSIBLE PARTY}} {{TRAVEL EXPENSE REIMBURSEMENT CONDITIONS}}.

Signatures

All parties, by signing below, accept and agree to the terms listed above and in all referenced
documents throughout:

{{RECIPIENT REPRESENTATIVE NAME}}:

_____

{{ASSESSOR REPRESENTATIVE NAME}}:

_____

Rules of Engagement

Scope of Work

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

- {{ACTIVITY WITHIN THE ENGAGEMENT}}
- {{ACTIVITY WITHIN THE ENGAGEMENT}}
- {{ACTIVITY WITHIN THE ENGAGEMENT}}
- {{ACTIVITY WITHIN THE ENGAGEMENT}}
- {{ACTIVITY WITHIN THE ENGAGEMENT}}
- Additionally, the {{ASSESSOR DESIGNATED CONTACT}} will hold meetings with the {{RECIPTIENT DESIGNATED CONTACT}} , {{MEETING FREQUENCY}}, to inform them of the overall progress of the assessment.

For each phase, the Assessor will to combine research, interaction with key staff members, larger facilitated exercises, and where appropriate, technical verification/investigation to achieve a comprehensive understanding of the organization's potential risks.

Assumptions and Limitations

- The Assessor has the experience and ability to do everything agreed to for Recipient and will do it all in a professional and timely manner. The Assessor will endeavor to meet every deadline and perform the Engagement in accordance with the sector's best practices.
- The Assessor 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 the assessors 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 the Assessor 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 the Assessor will guide them through the setup and use of the tools required.

Engagement Schedule

The Assessor will adhere to the following schedule

- The {{ACTIVITY WITHIN THE ENGAGEMENT}} will begin and will last {{LENGTH OF TIME ACTIVITY WILL TAKE}}.
- The {{ACTIVITY WITHIN THE ENGAGEMENT}} will begin and will last {{LENGTH OF TIME ACTIVITY WILL TAKE}}.
- The {{ACTIVITY WITHIN THE ENGAGEMENT}} will begin and will last {{LENGTH OF TIME ACTIVITY WILL TAKE}}.
- The {{ACTIVITY WITHIN THE ENGAGEMENT}} will begin and will last {{LENGTH OF TIME ACTIVITY WILL TAKE}}.
- The {{ACTIVITY WITHIN THE ENGAGEMENT}} will begin and will last {{LENGTH OF TIME ACTIVITY WILL TAKE}}.

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 {{INCIDENT DISCLOSURE PERIOD}}.

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
{{CONTACT NAME}}	{{CONTACT NUMBER}}	{{CONTACT SECURE CONTACT}}
{{CONTACT NAME}}	{{CONTACT NUMBER}}	{{CONTACT SECURE CONTACT}}
{{CONTACT NAME}}	{{CONTACT NUMBER}}	{{CONTACT SECURE CONTACT}}

Assessor Contacts

Full Name	Phone Number	Secure Channel

Assessor 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 the Assessor will mitigate, to the extent practicable, the harmful effects of the

security incident that are known to the Assessor; and document security incidents and their outcomes.

Privacy and Security

Privacy and Security

- All Engagement findings, results, and recommendations are confidential and will be treated as such.
- Assessor 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.

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

Safeguards to Protect Confidential Data and Communications

Device Security

The Assessor will secure all the devices they will use for the assessment. This includes

- {{DEVICE SECURITY PRACTICE}}
- {{DEVICE SECURITY PRACTICE}}
- {{DEVICE SECURITY PRACTICE}}

Communications Security

It will often be essential that confidential information be shared between the Recipient and the Assessor. 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 the Assessor. The Assessor will destroy the above hardcopy documents using the destruction practices described below.

The Assessor will destroy all confidential material {{DATA RETENTION PERIOD}} after the Engagement.

When destroying confidential material the Assessor will permanently delete all electronic data from all Assessor' 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.

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

Party	Full Name	Signature
Recipiant	{{CONTACT NAME}}	
Recipiant	{{CONTACT NAME}}	
Recipiant	{{CONTACT NAME}}	

Signatures

By signing this document, {{RECIPIENT REPRESENTATIVE NAME}} gives {{ASSESSOR REPRESENTATIVE NAME}} permission to conduct a security assessment.

By signing this document, {{ASSESSOR REPRESENTATIVE NAME}} agrees to adhere to scope provided while running this Assessment. {{ASSESSOR REPRESENTATIVE NAME}} also agrees to adhere to the terms and conditions aforementioned in this document.

{{RECIPIENT REPRESENTATIVE NAME}}:

_____

{{ASSESSOR REPRESENTATIVE NAME}}:

_____