STATEMENT OF WORK

Project Name:	Pen Test	**Seller Representative:** Liam McNamara +1 (703) 262-8156 liammcn@cdw.com
Customer Name:	WILLIAMSON COUNTY, TX	
CDW Affiliate:	CDW Government LLC	
Date:	August 02, 2022	**Solution Architect:** Mikela Lea
Drafted By	Vincentia Kotoku	

This statement of work ("**Statement of Work**" or "**SOW**") is made and entered into on the last date that this SOW is fully executed as set forth below ("**SOW Effective Date**") by and between the undersigned, CDW Government LLC ("**Provider**," and "**Seller**,") and WILLIAMSON COUNTY, TX ("**Customer**," and "**Client**,").

This SOW is subject to the terms and conditions of the OMNIA Partners Region 4 Education Services Center "ESC" Contract #R210401 held by CDW Government LLC with an effective date of June 1, 2021 (the "**Agreement**"). If there is a conflict between this SOW and the Agreement, then the Agreement will control, except as expressly amended in this SOW by specific reference to the Agreement.

PROJECT DESCRIPTION

PROJECT SCOPE

The Rapid Security Assessment (RSA) is a security assessment designed to balance the need for thorough and reliable security testing with the demands of short timelines and limited budgets. During this assessment, we use commercially available vulnerability scanners, proprietary tools developed by our security engineers, and tools created by the open source community to identify and document existing weaknesses, and provide our advice for the remediation of vulnerabilities identified during the course of the engagement. Where appropriate, the engineers may exploit vulnerabilities in order to more accurately determine the risk to your environment. The RSA report is a hybrid of the engineers' observations of the current state of your network security and their interpretations of the data gathered by the scanners.

The RSA consists of up to four parts, as described below.

SCOPE OPTIONS

PART A: INTERNET SECURITY TESTING

The engineers will scan Internet-visible hosts, identify services running on the hosts, and conduct testing for vulnerabilities to known exploits. Test results will be manually validated, as necessary, in an effort to minimize false-positive reporting. Where appropriate, the engineers may exploit vulnerabilities in order to more accurately determine the risk to your environment. The Internet Test portion of the RSA offering is limited to 40 targets.

PART B: INTERNAL SECURITY TESTING

The Internal Assessment contains multiple tasks.

- **Internal Vulnerability Scan** - The engineers will scan your internal network, identify services running on the hosts, and conduct testing for vulnerabilities to known exploits. Test results will be manually validated, as necessary, in an effort to minimize false-positive reporting. The Internal Test portion of the RSA offering is limited to 1,000 targets.
- **Penetration Testing –** Penetration testing of key organizational IT assets will be performed, in an attempt to gain access to these key assets and provide documentation on the path to access.
- **Domain Security and Password Audit** – An audit of passwords and password-related policies used within the organization will be performed, with guidance provided on potential improvements. This item is limited to a single Active Directory domain.
- **Authenticated Scan** – Up to 50 workstations will be tested via an authenticated scan. The results of this scan, once validated, should provide a good snapshot of workstation security.

PART C: WIRELESS SECURITY TESTING

The engineers will scan the 802.11-based signal cloud around your network testing for ways that outsiders could eavesdrop on your wireless communications, break authentication or cryptographic protocols, or impersonate elements of your wireless infrastructure. The Wireless Test portion of the offering is limited to one physical site (the same site at which Part B will take place).

PART D: SOCIAL ENGINEERING PHISHING EXERCISE

Social Engineering is a process in which access is gained to a network using People, Process often combined with technology. Various types of social engineering can be used by a hostile party to exploit a network. Seller will only demonstrate non-malicious and non-harmful Social Engineering Techniques to demonstrate these possible vulnerabilities. We propose a Phishing Attack against the employees (computer users) of Customer network. The exercise will include the following items.

- Social Engineering & Phishing exploit against the users of users of Customer network.
- Email addresses can be mined from the Internet or Customer can provide list of the user email addresses.
- The collection of the responses will be provided within the report. Customer can designate if they want to include, or omit user names and password content in the report.

PROJECT KICKOFF – KEY ACTIVITIES

- IP Addresses to be scanned will be shared from Customer to Seller. Any addresses to exclude will be discussed. Any time-of-day exclusions to scanning will be discussed.
- For Part B, a pre-arranged time and date for an end to the penetration testing task will be discussed. If the engineers are unsuccessful in uncovering valid administrative credentials by this time, Customer will provide valid credentials at this prearranged time to allow the domain security and password audit and authenticated scan to be completed.

CUSTOMER RESPONSIBILITIES

1. For part A and B, Customer will provide Customer IP addresses to be scanned. By providing these addresses, Customer acknowledges permission for scanning and penetration testing to take place.
2. For part B, if the penetration test is unsuccessful in uncovering valid administrative credentials, Customer will provide valid credentials at a prearranged time to allow the domain security and password audit and authenticated scan to be completed.
3. Obtain any necessary permission for testing of systems hosted or managed by third parties.
4. Provide a point of contact for questions and updates about project status.
5. Respond to requests for information in a timely manner.

6. For part B and C, provide access to physical facilities, as needed.
7. For part B and C, provide appropriate workspace, including power and network access.
8. Agree to Seller's Supplemental Security terms and conditions that can be found on the attached Exhibit B (see sample attached)

PROJECT ASSUMPTIONS

1. **A target is defined to be a system to be scanned**. Often, there is a one-to-one mapping between an IP address and a target. However, there are situations, such as name-based virtual web hosting, where there are multiple targets that map to one IP address.
2. For part A, the number of Internet-facing targets to be scanned is capped at 40.
3. For part B, the number of internal targets to be scanned is capped at 1,000.
4. For part B, the domain security and password audit task is limited to a single Active Directory domain.
5. For part B, the number of workstations to be scanned during the authenticated scan is capped at 50.
6. For part B, the domain security and password audit as well as the authenticated scan require a level of privilege in the environment. It is the intent to acquire this privilege during the penetration test. However, if the necessary level of privilege is not gained, it is assumed that Customer will provide credentials at a pre-arranged time to allow these parts of the engagement to proceed. If the credentials are not provided in a timely fashion, the domain security and password audit and authenticated scan will be removed from the project's scope.
7. While rare, network scanning can potentially have an adverse effect on a host. It is understood that Seller bears no liability for any loss of service to a host during this engagement due to network scanning.
8. Assessment activities may include attacks against end-user clients, such as email-based attacks (where these attacks focus on technical issues rather than user behavior). Note that this does not include credential phishing unless phishing is specifically included in the project scope.
9. It is assumed that Customer's IT staff will be aware of Seller's assessment activities and will not actively interfere with or attempt to actively defend against Seller's attacks and assessment activities. Active interference by Customer staff in Seller's assessment activities may result in limited results from the assessment or a reduction in scope. In this event, a change order may be needed to increase the project cost and/or timeline in order to complete the full original scope of the assessment.
10. Project tasks will be completed during business hours (8am to 5pm, Monday through Friday).

OUT OF SCOPE

Tasks outside this SOW include, but are not limited to:

1. Systems outside of the United States. No work under this SOW will be performed on any systems outside of the United States.
2. Post-remediation scans or retesting of findings are out of scope for this project and may incur additional cost.

ITEM(S) PROVIDED TO CUSTOMER

The following will be provided to Customer by the completion of this project:

Rapid Security Assessment Report – The report outlines the efforts undertaken by the engineers and provides customized security findings and recommendations for improvement.

The report includes:

- An executive summary showing the effectiveness of your security controls,
- Summarized high-level recommendations and a rating of the overall risk of the environment.,
- An outline of the efforts made by the engineers, highlighting attacks that were successful or otherwise pose higher risks
- Summaries of more widespread issues, with detailed itemized lists of weaknesses presented when appropriate, and

- A section listing recommendations, ordered by priority and by the estimated cost to fix them, with high-priority, low-cost items at the top of the list.

Seller prides itself on the quality and usefulness of this report. Although automated scanners are used during the assessment, the report is not simply a reproduction of output from automated tools.

Due to the sensitive nature of this report, we will convey to you a password-encrypted file. Only members of our assessment team have access to the report.

Once we have delivered the report, we will solicit your feedback. If necessary, we will revise the report. Once the report is finalized, we will conduct a project wrap-up call to walk through the project one final time and ensure that any remaining questions are addressed.

Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

General Responsibilities and Assumptions

- Customer is responsible for providing all access that is reasonably necessary to assist and accommodate Seller's performance of the Services.
- Customer will provide in advance and in writing, and Seller will follow, all applicable Customer's facility's safety and security rules and procedures.
- Customer is responsible for security at all Customer-Designated Locations; Seller is not responsible for lost or stolen equipment, other than solely as a result of Seller's gross negligence and willful misconduct.
- This SOW can be terminated by either party without cause upon at least fourteen (14) days' advance written notice.

Contact Persons

Each Party will appoint a person to act as that Party's point of contact ("**Contact Person**") as the time for performance nears and will communicate that person's name and information to the other Party's Contact Person.

Customer Contact Person is authorized to approve materials and Services provided by Seller, and Seller may rely on the decisions and approvals made by the Customer Contact Person (except that Seller understands that Customer may require a different person to sign any Change Orders amending this SOW). The Customer Contact Person will manage all communications with Seller, and when Services are performed at a Customer-Designated Location, the Customer Contact Person will be present or available. The Parties' Contact Persons shall be authorized to approve changes in personnel and associated rates for Services under this SOW.

Change Management

This SOW may be modified or amended only in a writing signed by both Customer and Seller, generally in the form provided by Seller ("**Change Order**"). Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

In the event of a conflict between the terms and conditions set forth in a fully executed Change Order and those set forth in this SOW or a prior fully executed Change Order, the terms and conditions of the most recent fully executed Change Order shall prevail.

Project Scheduling

Customer and Seller, who will jointly manage this project, will together develop timelines for an anticipated schedule ("**Anticipated Schedule**") based on Seller's project management methodology. Any dates, deadlines, timelines or schedules contained in the Anticipated Schedule, in this SOW or otherwise, are estimates only, and the Parties will not rely on them for purposes other than initial planning.

The following scheduling scenarios that trigger delays and durations to extend beyond what's been planned may require a Change Order:

- Site preparation, such as power, cabling, physical access, system access, hardware/software issues, etc. must be completed in a timely manner.
- Project tasks delegated to Customer PMs/Engineers/Techs/Management/Resources must be completed in a timely manner. For example, in the event a project 's prioritization is demoted, and Customer resources are reallocated causing the project's schedule to extend on account of experiencing interruptions to its momentum requiring complete stop(s) and start(s).
- External projects/dependencies that may have significant impact on the timeline, schedule and deliverables. It is Seller's assumption that every reasonable attempt will be made to mitigate such situations.

TOTAL FEES

The total fees due and payable under this SOW ("**Total Fees**") include both fees for Seller's performance of work ("**Services Fees**") and any other related costs and fees specified in the Expenses section ("**Expenses**").

Seller will invoice for Total Fees. Customer will pay invoices containing amounts authorized by this SOW in accordance with the terms of the Agreement. Unless otherwise specified, taxes will be invoiced but are not included in any numbers or calculations provided herein. The pricing included in this SOW expires and will be of no force or effect unless it is signed by Customer and Seller within thirty (30) days from the Date list on the SOW, except as otherwise agreed by Seller. Any objections to an invoice must be communicated to the Seller Contact Person within fifteen (15) days after receipt of the invoice.

PAYMENT: Williamson County's payment for goods and services shall be governed by Chapter 2251 of the Texas Government Code. An invoice shall be deemed overdue the 31st day after the later of (1) the date Williamson County receives the goods under the Contract; (2) the date the performance of the service under the Contract is completed; or (3) the date the Williamson County Auditor receives an invoice for the goods or services. Interest chargesfor any overdue payments shall be paid by Williamson County in accordance with Texas Government Code Section 2251.025. More specifically, the rate of interest thatshall accrue on a late payment is the rate in effect on September 1of Williamson County's fiscal year in which the payment becomesdue. The said rate in effect on September 1 shall be equal to the sum of one percent (1%); and (2) the prime rate published in the Wall StreetJournal on the first day of July of the preceding fiscal year that does not fall on a Saturday or Sunday.

SERVICES FEES

Services Fees hereunder are FIXED FEES, meaning that the amount invoiced for the Services will be $28,600.00.

The invoiced amount of Services Fees will equal the amount of fees applicable to each completed project milestone (see Table below).

Table – Services Fees

Milestone	Percentage	Fee
Completion of Work	100%	$28,600.00
Totals	**100%**	**$28,600.00**

EXPENSES

Neither travel time nor direct expenses will be billed for this project.

Travel Notice

The parties agree that there will be no travel required for this project.

CUSTOMER-DESIGNATED LOCATIONS

Seller will provide Services benefiting the locations specified on the attached Exhibit ("**Customer-Designated Locations**").

SIGNATURES

In acknowledgement that the parties below have read and understood this Statement of Work and agree to be bound by it, each party has caused this Statement of Work to be signed and transferred by its respective authorized representative.

This SOW and any Change Order may be signed in separate counterparts, each of which shall be deemed an original and all of which together will be deemed to be one original. Electronic signatures on this SOW or on any Change Order (or copies of signatures sent via electronic means) are the equivalent of handwritten signatures.

CDW Government LLC	**WILLIAMSON COUNTY, TX**
By: Jeni Kapelinski Digitally signed by Jeni Kapelinski Date: 2022.08.02 13:03:49 -05'00'	By:
Name: Services Contracts Manager	Name:
Title: Services Contract Manager	Title:
Date:	Date:
Mailing Address:	Mailing Address:
200 N. Milwaukee Ave.	301 SE INNER LOOP STE 105
Vernon Hills, IL 60061	GEORGETOWN, TX 78626-8207

EXHIBIT A

CUSTOMER-DESIGNATED LOCATIONS

Seller will provide Services benefiting the following locations ("**Customer-Designated Locations**").

Location(s)	Address
Main	301 SE INNER LOOP STE 105, georgetown, TX 78626

EXHIBIT B

SECURITY SERVICES SUPPLEMENTAL TERMS

PLEASE READ THESE TERMS AND CONDITIONS VERY CAREFULLY.

CUSTOMER AGREES TO BE BOUND BY AND ACCEPTS THESE SUPPLEMENTAL TERMS AND CONDITIONS.

1. Customer acknowledges and agrees that it understands and accepts the risks associated with the Services and hereby expressly authorizes Seller to perform the Services.

2. Customer represents, warrants and covenants that: (a) it has and will continue to have full rights, power, and authority to consent to having the Services provided in the manner as agreed upon in the SOW; (b) the execution and performance of the SOW does not and will not violate or constitute a default under its constituting documents or any applicable law, any order of any court or government agency, or any agreement to which it is a party; (c) the execution and performance of the SOW has all been duly and validly authorized by all necessary corporate action, and the SOW and/or Agreement constitute a valid and binding obligation of Customer; (d) it holds all permits, licenses, approvals and statutory authorities that are necessary for the performance of its obligations under the SOW, including, but not limited to, any approvals or consents, or providing any notices, required under applicable laws in respect of the processing of any personal data, and it has obtained in writing all consents, approvals and licenses necessary (including, but not limited to, from any third party) to allow: (i) Seller, its affiliates, subcontractors and its or their personnel to provide the Services; (ii) Customer to receive the Services; and (iii) for the Seller, its affiliates, subcontractors and its or their personnel to be able to access and test the Customer's communications network, systems, applications and equipment, including, without limitation, any third party provided, supplied, licensed, hosted or managed network, systems, applications, equipment and/or elements of the same ("Customer's Network"), in the manner detailed in the SOW; (e) Seller's performance of the Services as anticipated under the SOW will not cause Seller, its affiliates, subcontractors and its or their personnel to commit any offence under any relevant computer misuse, cyber-security, anti-hacking, wire-tapping, interception of communications or systems, or similar or related legislation, regulation or binding industry code, guidance or requirements in any country (including where the services are provided, performed, received or relevant IT equipment, assets and/or systems are located) ("**Computer Misuse Legislation**") and Customer has provided its consent in relation to the Services and has obtained all required consents in respect of the same; and (f) it will use the Services for lawful purposes only. Seller shall not be liable for claims resulting from a breach of any of the foregoing.

3. Customer acknowledges and agrees that:

    a. the Services include investigating and exploiting the Customer's Network and security vulnerabilities by attempting to gain access to Customer's Network and confidential security-related information through testing activities that are not authorized by Customer's Network security policies and that if done without Customer's and/or the applicable third party's authorization and consent could violate applicable laws;

    b. the Services relating to security are only one component of Customer's overall security program and are not a comprehensive security solution or a comprehensive evaluation of Customer's security and, without limiting the foregoing (a) it is impossible to, and the Services will not, detect, disclose or resolve every security vulnerability or hazard, (b) unauthorized access by third parties may occur and (c) impenetrable security cannot be attained; and

    c. Seller may perform any or all of the Services either directly or by using subcontractors or any other authorized personnel, in its sole discretion.

4. Customer is, and will continue to be, solely responsible for:

a. exercising reasonable care under the circumstances in monitoring and managing its security environment and mitigating the risks associated with any potential or actual security hazard;

b. establishing and maintaining appropriate internal controls and complying with all applicable laws and regulations;

c. implementing any advice or recommendations provided by Seller as part of the Services.

5. Customer represents and warrants that it owns all right, title, and interest in and to, or has the license for and the right to grant Seller access to and to authorize Seller to bypass or attempt to bypass any security features or technological protection measures associated with, any programs, systems, hardware, data, materials, IP addresses, domains or other information furnished or made available by Customer to Seller for the purpose of enabling Seller to perform the Services. Customer hereby assumes the sole responsibility for the accuracy of such programs, systems, data, materials, IP addresses, domains or other information furnished or made available by Customer to Seller.

6. Customer shall cooperate with Seller in the performance of the Services. Without limiting the previous sentence, Customer shall: (a) provide Seller, its affiliates, subcontractors and its or their personnel with timely access to the Customer's Network, the Customer's data and information reasonably requested by Seller with respect to the Services; (b) promptly render all decisions and approvals so as not to delay or impede Seller's performance of the Services; and (c) promptly notify Seller of any issues, concerns or disputes regarding the Services. Customer acknowledges and agrees that Seller's performance depends on Customer's timely and effective satisfaction of Customer's responsibilities under the SOW and/or Agreement and Customer's timely decisions and approvals in connection with the Services.

7. Customer shall permit, and hereby authorizes, Seller to connect diagnostic software and equipment to Customer's Network for the purposes of performing the Services, which may require accessing Customer's Network and confidential security-related information. Seller has no liability or obligation for: (a) the installation, operation or maintenance of the Customer's Network; or (b) the availability, capacity or condition of the Customer's Network or (c) any adverse impact of the Services on the Customer's Network.

8. Customer and Seller acknowledge and agree that, in connection with Seller's performance of the Services,

   Seller is not required to access, process or transfer data that identifies or can be used to identify a natural person ("**Personal Information**").
   a. Seller is acting as a service provider, and is neither a controller nor owner of Personal Information;
   b. to the extent data accessed or processed by Seller constitutes Personal Information, that Personal Information will be accessed or processed based on Customer's direction, and Seller has no rights to use that Personal Information other than in connection with providing the Services to Customer;
   c. Customer is solely responsible for obtaining any approvals or consents, or providing any notices, required under applicable laws regarding Seller's performance of the Services, including, but not limited to, the processing of any Personal Information.
9. Customer shall identify Customer's mission-critical systems for Seller, and Seller will discuss appropriate testing for these systems. Seller shall have no liability or responsibility with respect to such systems when testing is authorized.

10. Notwithstanding anything to the contrary in the SOW and/or Agreement, Customer shall be solely responsible for daily back-up and other protection of data (including, but not limited to, any data of Customer, Customer's customers, Customer's contractors and any other third party) and software against loss, damage or corruption. Customer shall be solely responsible for reconstructing or restoring such data (including, but not limited to, data located on disk files and memories) and software that may be lost, damaged or corrupted during the performance of the Services. Customer shall perform a full back-up prior to Seller commencing the Services and shall also perform the same periodically

throughout the delivery of the Services. Customer shall be solely responsible for ensuring proper and adequate backup and storage procedures.

11. Notwithstanding anything to the contrary in the SOW and/or Agreement, Seller warrants that it will perform the Services in a professional manner that is consistent with industry practice. Customer acknowledges and agrees that Customer's exclusive remedy for any breach of this warranty will be for Seller, upon receipt of written notice by Customer, to use reasonable efforts to cure that breach. Except as expressly set out in the Agreement, Seller makes no, and expressly disclaims all, representations, warranties or conditions, whether express, implied or statutory, including, but not limited to, warranties of merchantability, fitness for a particular purpose, title, non-infringement, quiet enjoyment or from a course of dealing, course of performance or usage in trade in connection with the Services. Seller does not warrant, and specifically disclaims, that the Services will be accurate, without interruption or error-free.

12. NONE OF SELLER, ITS AFFILIATES, THEIR RESPECTIVE SUPPLIERS, SUBCONTRACTORS, EMPLOYEES OR AGENTS SHALL BE LIABLE TO CUSTOMER OR TO ANY THIRD PARTY FOR, AND CUSTOMER WILL BE RESPONSIBLE FOR, ANY CLAIMS, LIABILITIES, LOSSES, DAMAGES, COSTS OR EXPENSES (INCLUDING, BUT NOT LIMITED TO, LEGAL FEES AND EXPENSES) RESULTING FROM, ATTRIBUTABLE TO OR ARISING OUT OF CUSTOMER'S USE OR RECEIPT, OF THE SERVICES (INCLUDING, BUT NOT LIMITED TO, IN CONNECTION WITH THE LOSS, DAMAGE OR CORRUPTION OF DATA AND SOFTWARE). THE FOREGOING SHALL APPLY IN ADDITION TO AND NOTWITHSTANDING ANY OTHER DISCLAIMER OR

    LIMITATION OF LIABILITY OTHERWISE CONTAINED IN THE SOW AND/OR AGREEMENT.
13. IN NO EVENT SHALL SELLER BE LIABLE TO THE CUSTOMER FOR ANY:

    a. LOSS OF GOODWILL, PROFITS, USE OF MONEY, BUSINESS OR REVENUE (WHETHER DIRECT OR INDIRECT);
    b. LOSS OF USE OF, INTERRUPTION IN USE OR AVAILABILITY OF, HARDWARE OR SOFTWARE;
    c. LOSS OF, OR DAMAGE TO, OR CORRUPTION OF, OR INTERRUPTION IN USE OR AVAILABILITY OF, DATA (WHETHER DIRECT OR INDIRECT) ;
    d. STOPPAGE OF OTHER WORK OR IMPAIRMENT OF OTHER ASSETS; AND/OR
    e. INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIALDAMAGES, WHETHER BASED ON BREACH OR FAILURE OF EXPRESS OR IMPLIED WARRANTY, BREACH OF CONTRACT, MISREPRESENTATION, NEGLIGENCE, TORT, STRICT LIABILITY IN DELICT OR OTHERWISE, ARISING FROM OR RELATED TO THE SOW AND/OR AGREEMENT, ANY COMMITMENT PERFORMED OR UNDERTAKEN UNDER OR IN CONNECTION WITH THE SOW AND/OR AGREEMENT, THE SERVICES OR OTHERWISE, REGARDLESS OF WHETHER SELLER HAS BEEN ADVISED, KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.
14. THE AGGREGATE CUMULATIVE MONETARY LIABILITY OF SELLER UNDER OR RELATING TO THE AGREEMENT SHALL NOT EXCEED THE AMOUNTS PAID OR PAYABLE BY THE CUSTOMER TO SELLER FOR THE SERVICES GIVING RISE TO THE CLAIM.

15. The following indemnification obligations of the Customer are cumulative and shall apply in addition to any other indemnification obligations of the Customer set out in the SOW and/or Agreement:

    a. Customer agrees to defend, indemnify and hold Seller and its affiliates and their respective directors, officers, members, employees, contractors, representatives, successors and assigns (collectively the "**Indemnified Parties**") harmless from and against any loss, damage, liabilities, cost, expense (including, but not limited to, legal fees and costs), claims, demands, fines, penalties or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including, without limitation, legal fees and expenses,

costs related to mitigation and equitable relief), claimed against or incurred by any of the Indemnified Parties as a result of, arising out of or otherwise related to:

i. a breach by Customer of any of Customer's obligations, responsibilities, covenants or warranties in the SOW and/or Agreement;

ii. any of Customer's representations in the SOW and/or Agreement being untrue;

iii. any prosecution under or breach arising out of the Computer Misuse Legislation related to performance of the Services; and/or

Customer agrees to defend, indemnify and hold the Indemnified Parties harmless from and against any loss, cost, expense (including, but not limited to, legal fees and costs), claims, demands, liabilities, fines, penalties, damages, or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including, but not limited to, legal fees and expenses, costs related to mitigation and equitable relief), claimed against or incurred by Indemnified Party based on, resulting from, arising out of or otherwise related to Customer's use or receipt of the Services.

b. Seller has the right to immediately terminate the Services upon written notice to Customer, without liability to Customer for such termination, if Seller determines that the performance of any part of the Services would be in conflict with law.