

Onboarding Agreement

This Supplier Agreement ("Agreement") is made on _____ ("Effective Date") by and between _____ (together with its corporate affiliates, "WL") and _____, a _____ corporation with offices at _____ ("Supplier").

In consideration of the mutual promises, covenants and agreements contained herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties, intending to be bound hereby, agree as follows:

TABLE OF CONTENTS

WL's Procurement requires you to review and complete the following documents in order to become a WL supplier. This Supplier Agreement contains the required terms and conditions to be a WL supplier.

SECTION I.	GENERAL CONDITIONS: A. ORDER PROCESSING, TERM & TERMINATION AND INVOICING B. THIRD PARTY SUPPLIERS
SECTION II	INSURANCE REQUIREMENTS
SECTION III	REGULATED PRODUCTS & MATERIALS (RPM) SPECIFICATIONS
SECTION IV	SAMPLE STATEMENT OF WORK ("SOW")
SECTION V	SUPPLIER ACKNOWLEDGEMENT

This document contains information from WL or its Affiliate companies, which may be confidential, privileged or otherwise protected from disclosure. This information is intended for use solely by the recipient(s) named. If you are not the intended recipient, be aware that any review, disclosure, copying, distribution or use of these contents is prohibited. If you have received this transmission in error, please immediately notify WL. "Affiliates" means any company or entity that is controlling, controlled by or under common control of either party. "Controlling", "Controlled By", or "Under the Common Control with" means either the beneficial ownership under trust, or outright ownership of more than fifty percent (50%) of the affiliate or business entity itself or the affiliate's or business entity's securities, or units if a limited liability company.

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

SECTION I.

GENERAL CONDITIONS

A. PROCESSING, TERM & INVOICING

WL Purchase Orders: Supplier acknowledges that they will not start production or provide a service without a valid purchase order # or executed statement of work (each an “Order”) from WL.

WL Payment Terms: As full consideration for satisfactory performance of the Services by Supplier, WL (or the Affiliate specified on the Order executed by such Affiliate) shall pay Supplier’s invoice amount not later than terms defined below following WL’s receipt of said invoice. Payment by WL or Affiliate of any such invoice shall constitute full and complete satisfaction of any and all actual and potential fees for the billing period covered by the invoice.

As full consideration for Supplier’s satisfactory provision of the products or performance of the services, WL will pay undisputed invoiced amounts within ninety (___) days, plus payment processing time, after receipt of timely, accurate and proper invoices. Contractor will not be entitled to payment for invoices submitted more than one hundred-and-eighty (180) days after WL’s receipt of Goods and/or Services.

Term And Termination: This Agreement is effective upon the Effective Date, and shall, except as expressly stated herein, remain in full force and effect for a period of _____ year(s) from the Effective Date (the “Initial Term”), and shall renew automatically on a year-to-year basis thereafter (each such annual period being a “Renewal Term”) unless either party (a) provides written notice of termination not less than Ninety (90) days prior to the end of the Initial Term or any Renewal Term or (b) terminates this Agreement in accordance with the terms herein.

B. THIRD PARTY SUPPLIERS

Subject to paragraph 21 of the Terms and Conditions, Supplier may not assign, delegate, subcontract or transfer any Order, the work required to be done or any payments to be made hereunder without WL’s prior written approval.

List all 3rd Party Suppliers you intend to use to support business with WL
(enter n/a on first line below if not applicable)

Supplier Name	Location	Products & Services

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

SECTION II.

INSURANCE REQUIREMENTS

CERTIFICATE OF INSURANCE (COI)

Minimum Levels of Insurance Coverage all suppliers shall maintain to conduct business with WL.

1. INSURANCE

- a. Required Coverage** – Supplier agrees to maintain the following types of insurance coverage during the term of this Agreement with insurance carriers rated “A VII” or better by the then current edition of Best’s Insurance Reports published by A.M. Best Company and licensed to do business in the state(s) in which the Products are produced, and the Services are performed:
- Workers' Compensation insurance as required by law in the state(s) where the Products are produced and the Services are being performed, including a waiver of subrogation in favor of WL and, if Supplier is an employment agency and temporary labor service provider, an Alternate Employer’s Endorsement;
 - Employers' Liability and Occupational Disease insurance with limits of \$500,000 per occurrence;
 - Commercial General Liability insurance with combined single limits of not less than \$2,000,000 per occurrence, including coverage for (1) premises and operations liability; (2) broad form property damage including damage to property in Supplier's care, custody or control; (3) blanket contractual liability; (4) personal and advertising injury; and (5) products and completed operations; If the Supplier is providing catering services, Supplier shall carry Liquor Liability insurance in addition to the General Liability coverage. If the Supplier is providing security services, Supplier shall include an Assault & Battery extension to the General Liability coverage,
 - If automobiles are used in connection with work to be performed hereunder, Commercial Automobile Liability insurance, covering all owned or rented vehicles, each with combined single limits of not less than \$1,000,000 per occurrence for bodily injury and property damage;
 - Motor Cargo Liability coverage with a limit not less than \$250,000 per conveyance;
 - Professional Liability Insurance with limits of \$1,000,00 or greater per occurrence; and
 - Cyber risk insurance, that includes, but is not limited to, network security and privacy liability with a minimum limit of \$2,000,000 per occurrence.
- b. Additional Requirements** - The Commercial General Liability and Automobile Liability policies will name WL as an additional insured as its interest may appear, and contain a cross liability (severability of interests) clause. The Commercial General Liability and Automobile Liability insurance shall be written on an occurrence basis.
- c. Insurance Certificates** – Supplier shall maintain certificates of insurance evidencing such insurance signed by an authorized representative of the insurance company. Such insurance shall provide that in the event of any material change in coverage or cancellation, at least thirty (30) days prior written notice shall be provided to WL. Supplier's insurance shall be primary and non-contributory to any insurance coverage maintained by WL. Supplier shall be responsible for deductibles, self-insured retentions and premium payments contained in any of the foregoing policies. If requested, properly endorsed Certificates of Insurance may be sent to WL.
- d. Subcontractors** – Any subcontractor that Supplier shall retain to perform Services under this Agreement must maintain insurance that meets all requirements of Supplier.
- e. Liability** – WL shall not, because of accepting, rejecting, approving, or receiving any certificate of insurance required hereunder, incur any liability for: the existence, non-existence, form or legal sufficiency of the insurance described on such certificate; the solvency of any insurer; or the payment of losses. No provision under this Section III shall be construed or deemed to limit Supplier’s obligations under this Agreement to pay damages or other costs and expenses.
- f. Supplier’s Tools and Equipment** – Supplier's own tools and equipment shall be entirely at Supplier's risk. Loss of WL property shall be at WL's risk unless the negligence of contractor or its subcontractors cause damage.

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

SECTION III.

REGULATED PRODUCTS & MATERIALS (RPM) SPECIFICATIONS

Acknowledgment

By signing below, Supplier represents and acknowledges that it has read and understood the foregoing requirements and that these Regulated Products and Materials Specifications may be updated from time to time by WL. Updated versions will be issued with advance notice.

Responsibility and Expenses - If a recall or other corrective action of a Regulated Product, or product made with Material from Supplier, is necessitated by a defect, failure to conform to Laws or Specifications or any other reason, or either party reasonably determines that a voluntary recall or other corrective action is merited, Supplier shall bear all actual and direct costs and expenses of such recall or other corrective action, including without limitation, costs of notifying customers, customer refunds, costs of returning goods, and other expenses incurred to meet obligations to third parties. Supplier shall hold harmless and indemnify WL and its customers from and against all such actual and direct expenses related to any such recall or other corrective action, including but not limited to, the actual cost of the Regulated Product or Material, as well as the costs of inspection, investigation, testing, replacement, customer accommodations, retrieval, segregation, storage, transportation, destruction or disposal, the costs of notification to customers and governmental agencies, the costs of record-keeping, call centers and other administration fees and attorney and consultant's fees incurred with respect to any recall or other corrective action. Additionally, Supplier shall indemnify, defend and hold harmless WL its customers and their respective affiliates, and their employees, directors, officers, agents and principals from and against any and all third party claims or demands for damages, suits, liabilities, reasonable fees and expenses of attorneys and other experts, penalties, court costs, and other expenses arising from the recalled or corrected Regulated Product or product made with Material from Supplier.

The version governing any Services Agreement signed by WL and Supplier shall be the version most current at the time a Purchase Order is issued to Supplier. WL shall retain copies of all versions of the documents referenced above during the term of the Services Agreement and records showing the effective dates of each version.

Supplier's Legal Company Name: _____

Signature:

Name:

Title:

Date:

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

SECTION IV.

SAMPLE STATEMENT OF WORK

This Statement of Work No. _____ (“**SOW**”) is by and between _____ (“**WL**”) and _____ (“**Supplier**” or “**Contractor**”) and is issued pursuant to, incorporates, and is governed by the _____ (“**Agreement**”) between the parties dated _____, and sets forth the specific terms and conditions relating to the provision of Services referred to in this SOW. The combination of the terms of the Agreement and the provisions of this SOW shall together constitute the contract between the parties in respect of the Services. To the extent that there is a conflict between the SOW and the Agreement, the Agreement shall prevail.

1. INTRODUCTION.

Effective Date for SOW No. _____

2. PROJECT SCOPE

This section provides a general definition of the scope of the project.

3. PROJECT OBJECTIVES

This section provides a statement of what is to be accomplished. This section should describe the requirements, expectations and objectives of the parties.

4. PROJECT SERVICES

5. CONTRACTOR RESPONSIBILITIES

This section describes Contractor’s responsibilities, if any, for accomplishing actions beyond those described in the preceding section.

6. WL RESPONSIBILITIES

This section describes WL’s responsibilities, if any, for accomplishing actions that may affect Contractor’s ability to deliver the Services or complete the project.

7. PRIMARY CONTACTS/NOTICE ADDRESSES

If to Supplier, to: _____

If to WL, to: _____

This section states the names of the individuals responsible for coordinating contact between WL and Contractor regarding the project. This section should also list the appropriate mailing addresses of the parties for purposes of receiving written notices under the Agreement.

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

8. PROJECT SCHEDULE AND TERM
9. PROJECT FEES
10. IMPORTANT NOTE

This SOW shall become effective on the Effective Date specified above and shall continue in effect until all Orders subject hereto have expired or been terminated.

IN WITNESS WHEREOF, the parties have executed this Statement of Work in duplicate as of the dates written below.

Company Name: WL

Signature:

Name:

Title:

Date:

Supplier Name: _____

Signature:

Name:

Title:

Date:

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

SECTION V.

SUPPLIER ACKNOWLEDGEMENT

This is to verify that the document, **Supplier Agreement**, has been reviewed, completed, and accepted by Supplier as required for the sections indicated below.

Reminder: do not delete any sections of this document, rather enter "n/a" if not applicable.

SECTION	SECTION TITLE	I have reviewed the following sections (check box)
SECTION I	General Conditions	
SECTION II	Insurance Requirements (COI)	
SECTION III	Regulated Products & Materials (RPM) Specifications	
SECTION IV	Sample Statement of Work	
SECTION V	Supplier Acknowledgement & Supplemental Terms & Conditions (this page)	

Supplemental Terms and Conditions

Supplier shall comply with WL's Supplier Code of Conduct as posted at [Williams Lea official website](#) and adopt an internal control system to ensure compliance therewith. Upon request by WL, Supplier shall furnish WL with information on its compliance with the aforementioned code of conduct and assist in any audit being conducted by WL or its representatives.

For avoidance of doubt, if Supplier's Services include the receipt, storage, maintenance or processing of, or if Supplier is otherwise granted access to, Protected Health Information or Personal Information or is otherwise involved in the administration of certain Medicare-related products or services, the terms of Specification H-1 (located at <https://www.rrd.com/about/supplier-info/h1>) shall apply to such Services. The terms "Protected Health Information" or "Personal Information" are defined in Specification H-1.

Supplier shall comply with the terms and conditions attached at Schedule 1, Anticorruption, Schedule 2, Data and Information Security, and Business Continuity Requirements, and Schedule 3, Background Checks.

By executing this acknowledgement, we agree to be bound by all the terms, conditions and procedures specified within the documents.

Company Name: WL

Supplier Name: _____

Signature:

Signature:

Name:

Name:

Date:

Date:

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

Schedule 1 – Anticorruption and Antibribery

- (i) Contractor represents and warrants that it and its directors, partners, principals, officers and employees are familiar with the requirements of the Anticorruption Laws and that none of them has violated, or shall violate, the Anticorruption Laws. In particular, neither the Contractor nor any of its directors, partners, principals, officers or employees has offered, made, promised to make, authorized or ratified, and Contractor agrees that it shall not (and shall cause its directors, partners, principals, officers and employees not to) offer, make, promise to make, authorize or ratify, whether in connection with the transactions contemplated by this Agreement or any other transaction involving WL, any payment of money or gift of anything of value, directly or indirectly to any: (1) Government Official; (2) person or entity when such offer, payment, transfer, or promise would violate the laws of the country in which made or the laws of the United States; or (3) other person or entity while knowing or having reasonable ground to believe that any portion of those payments or transfers will be offered, made, or promised, directly or indirectly, to the persons referred to in clause (1) or (2) above, in order to obtain or retain business for or with, or to direct business to any person or to secure any improper advantage. “Government Official” means any (a) officer or employee of a government or government department, agency or instrumentality (e.g., state-owned or controlled enterprises); (b) public international organization (e.g., The World Bank); (c) person acting for or on behalf of any such government or department, agency, instrumentality or international organization; or (d) any political party or party official or any candidate for political office.
- (ii) If WL has reasonable grounds to believe that Contractor has violated the Anticorruption Laws, WL may in its sole discretion (1) suspend all payments to Contractor pending clarification to its satisfaction of the circumstances that gave rise to the concern, and (2) investigate Contractor and/or audit, or have a third party audit, Contractor’s books and records for the purposes of ascertaining whether any such violation has occurred. “Anticorruption Laws” means the U.S. Foreign Corrupt Practices Act (the “FCPA”), the U.K. Bribery Act 2010, similar laws against foreign bribery or any other anti-bribery or anticorruption laws applicable to Contractor.
- (iii) If, after the date hereof, Contractor or any of its officers, directors, partners, principals, employees or, to its knowledge, shareholders, intends to become a Governmental Official or an affiliate or associate of any Governmental Official it shall provide at least three days’ prior written notice to the WL, which shall have the right to terminate this Agreement forthwith and Contractor shall not thereafter be entitled to any further fee or payment hereunder from and including the date of termination; provided that such termination shall not affect the right of Contractor to payment for services rendered prior to such termination or to the extent otherwise required by applicable law.
- (iv) The WL shall be entitled to request that Contractor certify at any time or from time to time its compliance with the representations, warranties and covenants set forth in this Section, including as a condition to payment of any amount due to Contractor hereunder and to refuse payment of any such amount if the WL has reason to believe that any certification provided by Contractor is inaccurate. Contractor agrees to immediately notify WL if it violates any Anti-Corruption Laws in the performance of this Agreement.

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

SCHEDULE 2

INFORMATION AND PHYSICAL SECURITY REQUIREMENTS

Contractor may not use, disclose, sell, or share any WL Confidential Information for any purpose other than in the performance of the Services hereunder without the prior written consent of WL and will contractually require any subcontractor performing Services on behalf of Contractor to maintain the confidence of such data. Contractor represents and warrants it will comply with all applicable privacy, data, information security or use laws, rules, and/or regulations that apply to Contractor's operations together with this Agreement.

Contractor will adhere to the Information and Physical Security Requirements below:

Network

- All Contractor devices processing WL Confidential Information must be located on a dedicated logical network segment and where stated be logically separated from the general network via firewall
- Contractor must provide secure connection methods (point to point VPN, for example).
- Contractor must ensure that all the Systems and applications operated by Contractor and/or its sub-contractor/sub processors that support WL Services(s) are protected from inbound and outbound network threats.
- Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access.
- Contractor must Identify, Protect, Detect and Respond to any security alerts and breaches.
- Contractor must maintain an up-to-date inventory of all of the organization network boundaries, including a network diagram, and must review it at least annually.
- Contractor must review its internal and external firewall rules at least annually.
- Contractor must maintain a capability to detect and protect against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- External connections to the Contractor network are documented, verified and approved prior to the connections being established to prevent security breaches.
- Contractor networks must be protected through applying defense-in-depth principles (e.g. network segmentation, firewalls, physical access controls to network equipment, etc.).
- Contractor must have network intrusion prevention technologies to detect and prevent malicious traffic for all inbound/outbound traffic and update signature databases in line with industry best practice and apply updates from the solution provider in a timely manner.
- Network connection between interoffice/ cloud service provider/ data centers must be encrypted over secure protocol.
- Contractor's wireless access to the network is subject to authorization, authentication, segmentation and strong encryption protocols.

Logical Access

- Access to WL Confidential Information must be provided on a least privilege basis
- Passwords to accounts should be changed at least every 60 days and should be different from the previous twelve (12) passwords.
- Passwords must be locked after five (5) unsuccessful logon attempts and allowed to re-attempt authentication after 30 minutes.
- Passwords must contain at least 8 characters made up of 3 of 4 below:
 - Uppercase letter
 - Lowercase letter
 - Numerical digit
 - Special Character

Contractor must maintain an up to date and correct record of its employees and subcontractors accessing WL Confidential Information.

Contractor must perform an access review of all Contractor employees and subcontractors providing Services, including administration of the infrastructure and applications within the scope of the Services on a quarterly basis.

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

Contractor will disable accounts/credentials of employees and subcontractors providing Services to WL upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) immediately but no more than twenty-four (24) hours.

Contractor must ensure secure multi-factor authentication for all instances of remote access to Confidential Information.

Data Management

- Contractor must ensure that all staff and subcontractors with direct access to Confidential Information are blocked from access to email and access to the Contractor network is blocked from personal mobile devices
- All systems used for development and testing must be located in a non-production environment and segregation of duties enforced at all times. There must be no live data in the development and test environment(s).
- All Confidential Information must be backed up. Backups must be stored offline in an encrypted format, and deleted once the agreed retention period is expired
- Contractor must use technical controls to secure WL Confidential Information from leakage/exfiltration and include but not limited to the following methods:
 - Unauthorized transfer of information outside the internal network/ Supplier network
 - Email
 - Internet / Web Gateway (including online storage and webmail)
 - Unauthorized transfer of Information to portable media
 - Insecure Information exchange with third parties (sub-contractors, sub-processors)
 - Inappropriate printing or copying of Information
 - Contractor must encrypt all WL Confidential Information in transit and at rest.
- Contractor must establish procedures to securely dispose WL Confidential Information using appropriate sanitization methods including but not limited to clearing, purging, and destroying for secure removal/erasure and recovery of WL Confidential Information from all storage media rendering WL Confidential Information irrecoverable in compliance with NIST 800 standards.
- At the completion of the Contractor's Services or at any time specified and requested by WL, Customer will no longer use, transfer or retain any copy of the WL Confidential Information in any form. And, without limiting the foregoing, Contractor will securely destroy and erase all copies of any WL Confidential Information (including copies and/or notes derived therefrom) in Contractor's possession or under Contractor's control upon written request of WL or pursuant to the applicable Order. For the avoidance of doubt, all WL Confidential Information is deemed Confidential Information. Contractor shall, upon WL's request, provide WL with a written certification of such destruction/purging signed by an officer of Contractor.
- No WL Confidential Information may be transmitted to, or processed outside of, the country from which it is provided to Contractor without the express written permission of WL.

Endpoints

- Contractor must ensure that the endpoints used for connecting to its network and WL Confidential Information must be configured securely with anti-virus software and critical updates applied monthly.
- Contractor endpoints must have fully encrypted hard drives.
- Only Contractor provisioned devices are authorized to access WL Personal Data. Personal devices are prohibited.

Vulnerability Management

- Contractor must have an established and effective vulnerability management program through established policies and procedures, and technical measures, for effective monitoring, timely detection and remediation of vulnerabilities within Contractor owned or managed applications, infrastructure network and system components.
- Contractor will conduct vulnerability scans using updated vulnerability signatures on at least a monthly basis.
- Contractor must remediate vulnerabilities based on risk rating: Critical 7 days; High 30 days; Medium 60 days.
- External penetration testing covering internet exposed devices and services within the scope of the Services must be conducted by a third-party penetration testing company on, at least, an annual basis. If requested, summary reports must be shared with WL.
- Contractor must have a patch management program with established policies and procedures to deploy the latest security patches to servers, network devices, applications, and endpoint devices

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

Log Management

- Contractor must have an implemented SIEM for the logging and monitoring, including detection and alerting, of suspicious activity using behavior and indicators of compromise triggers.
- Logs must be reviewed on at least a daily basis and events addressed immediately.

Security Incident Management

- Contractor shall maintain SOC2 Type II Certification during the Term of this Agreement and provide its SOC2 Type II audit report upon written request of WL.
- Contractor shall establish, test, and maintain an Information Security Incident response process that includes, among other things, processes for evidence preservation, informing and working with law enforcement agencies, government agencies and similar parties as appropriate, and performing forensic analyses;
- Contractor shall notify WL of any information Security Incident involving Confidential Information and/or WL Data, including any security incident at or involving Contractor's systems, hardware, equipment, devices or premises computers or otherwise involving Contractor's personnel. Contractor shall provide notification of any such security incident promptly, but in no event later than twenty-four (24) hours following the date Contractor first becomes aware of such Security Incident
- Contractor shall for each such Security Incident successfully resolved within twenty-four (24) from the time Contractor first becomes aware of such Security Incident, provide WL with a final written notification no later than three (3) days following Contractor's closure of such Security Incident, that includes detailed information regarding the root cause of such incident, actions taken, and plans to prevent a similar event from occurring in the future.
- Contractor shall in the event that system integrity cannot be restored within twenty-four (24) hours from the time Contractor concludes that a Security Incident has occurred provide WL with the following additional notice regarding the Security Incident, in a manner that does not publicly expose the existing vulnerability but enables WL, if possible, to take appropriate actions to mitigate its exposure or risk: (A) a confirmation that WL has been impacted by a Security Incident; and (B) a description of the Security Incident.
- Contractor will provide notification to WL promptly after the system integrity is restored and a report of the Security Incident has become available.
- WL will treat any notices from Contractor regarding a Security Incident as confidential information. Notwithstanding the foregoing obligation, if a Security Incident directly impacts WL's end customer or an Affiliate of WL, and notice is required, then WL may provide notice of the Security Incident to such impacted party.
- Following a Security Incident, Contractor agrees, at its own expense, to investigate the Security Incident and identify and mitigate the effects of the Security Incident. Contractor agrees to cooperate with any investigation of the Security Incident by WL, or agents acting on its behalf. WL agrees that such cooperation must be in a manner consistent with other contractual confidentiality requirements held by Contractor.
- "Security Incident" means (i) an actual disclosure or reasonable suspicion that there has been a disclosure, access, or loss of Confidential Information, Confidential Information or Protected Health Information held by Contractor to any unauthorized person or entity, or (ii) a condition where Contractor's Services present a potential security threat to WL or WL's end customer's network or systems, including the compromise of Contractor's email addresses and/or URLs.

Physical Security

- All standalone, co-located and third-party data centers, and cloud providers must be effectively secured to prevent unauthorized access and theft or damage to WL Confidential Information. All data centers must have layered technical, physical and manned controls and site-specific procedures in place to effectively protect the perimeter, building, and all other critical areas. Controls include, but are not limited to, security cameras, intruder detection systems, access control and security officers. Where installations are in shared locations, effective security around their discrete segregation must be deployed.

Subcontractors

- Contractor may not use any subcontractors, aside from those disclosed within this Agreement, without WL's approval. All information security requirements as identified within this Annex 2 must also be adhered by Contractor's subcontractors.
- Contractor must reassess each subcontractor at least annually for adherence to this Agreement.

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

Training

- Contractor employees must participate in a mandatory information security and privacy awareness training upon 90 days of hire and annually thereafter. The training should include, but not limited to, cybersecurity, anti-phishing, physical security, data privacy, and data management. Upon request, Contractor will provide WL with a copy of the training materials and/or records of employees' completion of training.

Audit Rights

- Contractor shall maintain on an annual basis appropriate externally verified information security, business continuity, and Quality Assurance certifications as required for the provision of the service (e.g. ISO 9001, ISO 27001, ISO 22301, SOC 2, PCI DSS). Upon request, Contractor will provide a copy of the most recent certifications.
- WL reserves the right to audit Contractor by means of questionnaire, phone interview and site visit at least annually.

Business Continuity Management

- Contractor shall develop and maintain a business continuity plan (operations and core business functions) and a disaster recovery plan (IT infrastructure / data recovery).
- Said plan will describe, in prudent detail, steps that Contractor and/or its agents, are to take to ensure Contractor's ability to perform its respective obligations under this Agreement. To ensure compliance with that concept, Contractor is to: (i) implement and maintain, for the duration of this Agreement, an adequate business continuity and disaster recovery plan, a copy of which will be provided to WL upon written request. (ii) cause its approved subcontractors, as applicable, to implement and maintain, for the duration of this Agreement, an adequate business continuity and disaster recovery plan, and Contractor will obtain documentation in support of all such plans and/or access thereto or obtain a copy of any third-party review of any such plan by a qualified independent party, pursuant to applicable industry standards; and (iii) notify WL of any material differences identified in any such plan or any significant changes that Contractor and/or its agents make to their respective plans that may have a serious, or material, effect on Contractor's ability to perform its duties under this Agreement.

Artificial Intelligence

- Contractor shall not use the Confidential Information, including Personal Data, in whole or in part, (1) for an unlawful purpose; (2) to distribute, share, sell, lease, license, exhibit, display, post, perform, make available publicly or privately, or otherwise transfer to any third party outside the performance of the Services; or (3) to train any artificial intelligence or machine learning engine or system, neural network, or similar system, absent a separate executed agreement expressly permitting these activities.

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0

SCHEDULE 3
BACKGROUND CHECKS:

Background check information is collected as a means of determining an applicant's ability to perform the particular Services and ensuring Contractor's employees performing services for or on behalf of WL are not a threat to the safety or security of our and our end customers' property or information. Each individual who is assigned to perform services for or on behalf of WL after the Effective Date shall be subjected to a background check, which is conducted by a third party vendor. The background check shall search for information starting from the date of the Effective Date or employment application (whichever is later). Therefore, Contractor, subject to Applicable Law, shall perform screening of any Contractor employee who will have access to WL Confidential Information. Such screening shall look back over the immediately preceding 7 years prior to employment with Contractor and include:

- Verify SSN / Comprehensive Address Verification (use of E-Verify)
- National Criminal Information Bureau Database (NCIB)
 - Includes National Sex Offender Registry
- Unlimited County Court Criminal / Statewide CrimeSearch

Contractor shall not permit the Services to be performed by any person who has been convicted of any offense involving dishonesty, breach of trust or duty, or money laundering that occurred in the preceding seven (7) years as well as any other criminal conviction that Contractor may reasonably determine poses a risk to the security of WL Confidential Information, having considered the nature of the conviction, the Services being provided, and any other relevant factors. If Contractor believes any person should be permitted to perform the Services notwithstanding the existence of an otherwise disqualifying criminal conviction, Contractor shall contact WL.

End customers may request that certain Contractor employees undergo a defined background check containing certain criteria not covered in the above-listed checks. WL shall inform Contractor in writing should such a defined background check be required.

Document Name:	Onboarding Agreement - Short				
Document #:	VM_2.12	Document Authorized by:	Global Head of Sourcing		
Issued / Revision Date:	12 Nov 2025	Revised by:	Global Procurement Team	Version #:	V 1.0