Product Terms

The following additional product terms ("**Product Terms**") apply when the Client purchases access to the Diligent Service which is identified in the Order Form as **Diligent HighBond** (or any module or application of the Diligent HighBond platform), **Robotics, RSAM, ACL for Windows, Analytics or Analytics Exchange (AX)**. Any references to "Diligent Services" in these Product Terms shall only refer to the products identified above.

For the purposes of these Product Terms capitalized terms used herein but not otherwise defined have the meaning given to them in the applicable Diligent General Terms and Conditions.

1. **Definitions**.

1.1. "**Client Systems**" means Client's own systems, infrastructure and personnel used to access and operate the Diligent Service, including, but not limited to, Client's servers, hardware, devices, data systems, internet connectivity, electric power, operating software and software applications (other than the Diligent Services).

1.2. "**Deliverables**" has the meaning given to it in Section 4.2.

1.3. "**Diligent Property**" has the meaning given to it in Section 4.2.

2. **Diligent Service.**

2.1. **Service Levels**. Diligent will make the applicable Diligent Services available in accordance with the service levels set out in the Service Level Agreement attached as Schedule "A" to these Product Terms. Client is responsible for providing and maintaining the Client Systems. Diligent will not be liable for any failures arising from or relating to the Client Systems.

2.2. **Client Support**. During the Subscription Term, Client will have access to support center to assist Client with its use of the Products. Basic support services (24x5) are included at no additional charge. Enhanced support services may be made available for purchase via Order Form. Support services are available via chat, email, telephone and the Diligent user community and are provided in accordance with the policies posted at www.wegalvanize.com/support-center, or such other url as Diligent may use for this purpose. Client will also have access to new releases and Updates of the Products when they become commercially available.

2.3. **Non-Production**. Any Diligent Service provided for non-production use, such as staging, testing, disaster recovery or failover, may only be used in a non-production environment and only for such non-production purposes.

2.4. **Demo License, Academic Use**. Any Diligent Service provided for demonstration purposes, or to a Diligent partner or for educational use (i.e. through the Academic Network Program or a textbook publisher) are provided "as is" without warranty and are used at Client's own risk. Diligent does not warrant the performance or security of such Diligent Service. The warranties, indemnities and remedies provided by Diligent under the Agreement do not apply to such Diligent Services.

Client Data - Security.

2.5. **Security Safeguards**. Diligent has implemented and will maintain the security safeguards set forth in the Security Schedule attached as Schedule "B" to these Product Terms. Client is responsible for assessing the suitability of such safeguards for the type of Client Data it uses in connection with the Diligent Service. Diligent will cooperate with Client to provide the information reasonably necessary for Client to assess the security of the Diligent Service, including completion of Client security assessments (no more than once annually) and providing Client with a copy of Diligent's current SOC 2 report in accordance with Schedule "B".

2.6. **Client Obligations**. Client is responsible for the security of its Client Systems and for the end-user security and access controls for its Diligent Service environment. Client will take reasonable security precautions in connection with its use of the Diligent Service as set forth in Schedule "B".

2.7. **Data Center.** Client Data stored in the Diligent HighBond platform is stored in the data center associated with Client's region based on the Client's address listed in the Order Form, unless the Client requests a different location in writing. Client Data stored in the RSAM platform is stored in the United States, unless the Client requests a different location in writing.

3. **Termination.**

3.1. **Data Retention Policy**. Client is responsible for determining its own data retention controls for Client Data and for deleting its Client Data from the Diligent Service. Diligent will allow access to the Diligent Service for a period of thirty (30) days after expiration or termination to facilitate such removal, which period may be extended by an additional thirty (30) days upon Client's written request. Following such period, Diligent will remove Client Data from the Diligent Service, however, Client Data may remain in back ups of the Diligent Service for up to one year. Upon Client's written request, Diligent will assist Client with the deletion of its Client Data from the Diligent Service.

3.2. **Effect of Expiration or Termination**. Upon expiration or termination of Client's subscription for the Diligent Service, in addition to Client's obligations under the Agreement, Client will destroy the original and all copies of any Software in its possession or control and if requested by Diligent, certify in writing to Diligent that the original and all copies of the Software have been destroyed or returned to Diligent within thirty (30) days of such written request.

4. **Additional Terms**

4.1. **Recurring Services**. If Client has purchased an annual allotment of hours of Professional Services, such hours may be used and drawn down on a time and materials basis throughout Client's annual subscription term for the Diligent Service. Each annual allotment of hours is non-transferable and will expire at the end of each annual subscription term if not used. Unused hours will not carry over to the following subscription term. If Client cancels its subscription to the applicable Diligent Service, all remaining hours will be forfeited at the time of cancellation.

4.2. **Ownership of Deliverables**. Notwithstanding Section 13.6 (Ownership) of the Agreement, unless otherwise provided in a Statement of Work, Client owns right, title and interest in and to any reports, documents or other materials created by Diligent specifically for Client as part of the Professional Services and provided as a deliverable of the Professional Services under a Statement of Work (the "Deliverables") in respect of the Diligent Service. To the extent a Deliverable includes any Diligent Property, upon payment of the fees for the applicable Deliverable, Diligent grants Client, during the applicable Subscription Term, a non-exclusive, worldwide, royalty-free license to use such Diligent Property in conjunction with the applicable Deliverable, and to modify such Diligent Property for Client's internal business purposes. Unless otherwise specified in a Statement of Work, Diligent is not required to maintain, support or otherwise repair any Deliverable or Diligent Property after its delivery to Client. "Diligent Property" means all scripts, analytics, compliance maps, frameworks, configurations, enhancements and derivative works of the Diligent Service or Software which are developed by Diligent either separate from or as part of the Professional Services.

4.3. **Impact Reports**. Any subscription that includes Impact Report(s) includes one (1) Impact Report and up to a maximum of forty (40) consulting hours during the 12 month subscription term to assist with creating the report template. Renewal subscriptions include up to eight (8) consulting hours during the 12 month subscription term to assist with maintenance and updating of Client's existing Impact Reports. Additional Impact Reports or hours can be purchased separately. Unused hours expire at the end of the subscription term and are not carried over. Consultants assisting with Impact Reports may require administrative access to Client's account from a region that is outside of Client's region (ie. Canada or India). Any additional consulting hours related to the Impact Reports included in a subscription above are subject to a statement of work entered into by parties which is governed by the terms of the Agreement.

4.4. **Non-Solicitation**. During the performance of any Professional Services and for a period of one (1) year after completion of such Professional Services, neither party will solicit, for the purposes of employment or retention as an independent contractor, any of the other party's employees or contractors involved in

providing the Professional Services. The foregoing will not prohibit either party from employing any individual who applies for a position in response to an internal posting, employment advertisement or other general solicitation of employment.

4.5. **Subcontractors**. Any subcontracting will not release Diligent from its obligations under this Agreement. Diligent will remain responsible for the work performed by its subcontractors to the same degree as if the work had been performed by Diligent itself. Upon written request, Diligent will identify to Client any subcontractors performing work in respect of this Agreement.

Schedule "A"
Service Level Agreement

This Service Level Agreement (**"SLA"**) applies to Diligent Service identified as HighBond (and its related modules and application), Robotics or RSAM in an Order Form. Capitalized terms used but not defined in this SLA have the meanings given to them in the Agreement.

1. **Service Level.** Diligent will use commercially reasonable efforts to make the Diligent Service operational and available to Client at least 99.9% of the time in any calendar month, excluding periods of Scheduled Maintenance (the **"Performance Commitment"**). If Diligent does not meet the Performance Commitment, Client will be eligible to receive the Service Credits described below. If Diligent fails to meet the Performance Commitment for three (3) consecutive calendar months during a subscription term, Client may terminate its subscription for cause. This SLA states Client's sole and exclusive remedy for any unavailability of the Diligent Service.

2. **Definitions.**

   a. "Downtime" means a period of at least ten (10) consecutive minutes during which the Diligent Service is unavailable and cannot be accessed or used. Intermittent interruption, downtime for a period of less than ten (10) minutes or unavailability of a Diligent Service caused by circumstances beyond Diligent's reasonable control (such as external forces affecting the reliability of the internet or Client's own systems or devices) will not be counted as Downtime. Downtime may be measured through an independent third party monitoring service selected by Diligent.

   b. "Monthly Uptime Percentage" means the Scheduled Service Uptime (as defined below) minus the total number of minutes of Downtime in a calendar month, divided by the Scheduled Service Uptime.

   c. "Scheduled Maintenance" means occasional maintenance of the Diligent Service to add resources, upgrade software, install security patches or carry out other routine maintenance procedures. Scheduled Maintenance typically occurs during the period of lowest anticipated system usage. System notification is provided in advance of Scheduled Maintenance. During Scheduled Maintenance, certain components of a Diligent Service may be offline, or may be operating in less redundant modes, or may be operating at reduced capacity levels.

   d. "Scheduled Service Uptime" means the total number of minutes in a calendar month (e.g., 43,200 minutes in a 30-day month) less the number of minutes of Scheduled Maintenance in such month.

3. **Service Credits.** If the Monthly Uptime Percentage for any calendar month is less than 99.9% and Client is impacted by any Downtime (ie, the Downtime occurs during regular business hours when Client is accessing a Diligent Service), Diligent will extend Client's subscription term, at no charge, by the applicable number of days noted in the table below.

Monthly Uptime %	Additional Subscription Days
< 99.9% - ≥ 99.0%	3 days
< 99.0% - ≥ 95.0%	7 days
< 95.0%	15 days

   To claim a Service Credit, Client must notify Diligent within thirty (30) days from the last day of the calendar month for which Client wishes to receive a Service Credit. No Service Credits will be issued after this thirty (30) day period. The maximum number of Service Credits available in any single calendar month is fifteen (15) days. Service Credits may not be exchanged for, or converted to, monetary amounts.

4. **Exclusions.** The Performance Commitment does not apply to, and no Service Credits are available for, any interruption or unavailability of the Diligent Service: (a) caused by factors outside Diligent's reasonable control, such as external forces affecting the reliability of the internet or any force majeure event; (b) that results from Client's actions or inactions or those of any employee, contractor, agent or third party acting on Client's behalf; (c) that results from Client Systems (as defined in the Agreement) or from any non-Diligent equipment, software or technology (other than third party equipment within Diligent's direct control); (d) Scheduled Maintenance; or (e) that results from a suspension or termination of Client's right to use the Diligent Service in accordance with the terms of the Agreement.

Diligent Security Schedule

This Security Schedule applies to the Diligent Service identified as Diligent HighBond (and its related modules and applications), Robotics and RSAM as identified in an Order Form and sets out the security for such Diligent Service. Capitalized terms used in this Schedule have the meanings given to them in the Agreement.

1. Shared Security Model

Security involves a joint effort by both Diligent and the Client. Diligent manages the overall security of the Diligent Service. The Client manages the end-user security and access controls for its Cloud Product environment and is responsible for determining the types of data to be used in connection with the Diligent Service.

2. Policies and Procedures

Diligent has implemented a security policy framework based on ISO 27001/2 to define minimum security requirements and expectations for security across its organization. The Diligent Service is supported by various operational and security policies, standards and procedures, including, but not limited to, those related to:

- Access Control
- Human Resources
- Change Management
- Information Classification
- Media Security
- Business Continuity
- Disaster Recovery
- Secure Software Development Lifecycle
- Vulnerability Management
- Security Incident Response
- Third-party Management
- Remote Access
- Logging and Monitoring
- Compliance

3. Security Measures

Diligent has implemented and will maintain commercially reasonable, industry-standard technical and organizational security measures designed to prevent the unauthorized access, use or disclosure of Client Data stored in the Diligent Service. Such security measures include, but are not limited to, the following:

a. Access Control. Diligent uses a principle of least privilege for internal administration. Access is granted on a need to know basis using a ticketing and approval system. Administrative access is protected with a combination of IP whitelisting, username/password, multi-factor authentication and private keys. Session limits for inactivity are set. All access is tracked and monitored for suspicious activity. Access to production system and internal applications is removed immediately upon personnel termination. Access rights are reviewed on a quarterly basis.

b. Personnel. Hiring practices ensure new personnel are qualified for their role. Background check procedures are in place for personnel who may have contact with Client Data. Personnel are required to complete annual security, confidentiality and privacy training upon hire and annually thereafter.

c. Data Encryption. Diligent provides encryption of data in transit and at rest. Encryption in transit is achieved via the industry-standard TLS (Transport Layer Security) protocol, including AES (Advanced Encryption Standard) with up to 256-bit key lengths. Encryption at rest is achieved by leveraging AWS storage encryption, which also relies on the AES encryption algorithm with strong 256-bit keys.

d. Physical Security. Diligent physical premises are kept locked during non-business hours and are protected by security guard and alarm services. Security cameras are visibly placed in high traffic or sensitive locations. Badges are required to gain entry into Diligent offices and must be visible at all times. Physical access is audited quarterly. Physical security at the data center is the responsibility of Amazon Web Services.

e. Network Security. Diligent uses a combination of web application firewalls, intrusion detection and prevention capabilities, as well as real time alerting. Diligent has developed procedures for monitoring Diligent HighBond systems for performance, availability, and security related events. These events are investigated promptly by the Diligent production operations team.

f. Hosted Environment. The Diligent Service is hosted by Amazon Web Services (AWS). Within the hosted environment, Client is provided with its own application environment (your Diligent service). AWS provides the physical facility and physical infrastructure of server hardware, networking and related services for the Diligent Service and the hosting of Client Data.

g. Asset Management & Endpoint Security. Information assets are classified and assigned in accordance with an asset management policy. Endpoint devices are managed through an endpoint management tool, including patches, encryption, anti-virus software updated at least once a day, and filtering malicious web content. Upon termination of personnel, laptops and building access cards are returned.

h. Penetration Testing. Diligent uses independent 3rd parties to perform regular penetration testing to check for security vulnerabilities, such as cross-site scripting, SQL Injection, session and cookie management. A summary of the most recent penetration test report can be made available to Client subject to the confidentiality provisions of the Agreement or a separate non-disclosure agreement.

i. Vulnerability Management. Vulnerability scanning is performed at least weekly for operating systems, software components, dynamic web applications, and static code analysis. All vulnerabilities are prioritized by severity using Common Vulnerability Scoring System. When possible, mitigations will be put in place for critical vulnerabilities while a full patch is being developed.

4. Backup and Disaster Recovery

Diligent maintains processes to ensure failover redundancy. In addition, full system/instance backups are taken on a regular basis for the purpose of restoring data integrity due to systemic or database failure, but not for purposes of restoring user deleted data. Backup media is encrypted and stored securely offsite. Diligent also maintains a Business Continuity Plan and Disaster Recovery Procedures.

5. Security Breach Procedures

Diligent maintains an Incident Response Plan managed by its Security Incident Response Team (SIRT). Diligent will notify Client without undue delay if Diligent determines that the security of the Diligent Service's systems has been breached and this results in Client Data being accessed by or disclosed to an individual or entity who is not authorized to access or receive such information. Notice will include a brief description of the incident, including the nature of the breach, the date it occurred and, if known, the general type(s) of data involved.

Diligent will report to Client on the corrective action being taken and will cooperate with Client to mitigate the effects of any lost or compromised Client Data. Diligent will conduct a root cause analysis to determine the cause of the incident and to ensure corrective actions are focused on the true root cause of the incident. Client will implement any corrective measures required by Diligent.

6. Client Security Obligations

Client controls the end-user security and access controls for its Diligent Service environment and manages the entire Client Data life cycle. Client determines what data to use, how long data should be retained, what data should be deleted, who can access the data, addition and removal of users, and configuration of system settings. Client is responsible for implementing appropriate security measures in connection with its use of the Diligent Service and its Client Data, including, without limitation, the following:

- use of security features made available through the Diligent Service
- establishing and enforcing use of strong passwords and setting password expiries
- establishing account access controls, such as configuring SSO (Single Sign On), challenging user accounts after multiple failed logins and using activity tracking to log access and system use
- setting session expiries
- specifically identifying permissible user IP addresses
- following industry best practices for de-identifying sensitive data
- backing-up Client Data
- limiting the type and amount of Client Data, as well as its storage, to only what is necessary for the intended purpose

Client will notify Diligent immediately if it becomes aware of any known or suspected breach of security related to its use of the Diligent Service.

7. Security Assessments

On Client's written request, Diligent will complete Client's reasonable security assessment questionnaire and provide Client with further information regarding the security measures for the Diligent Service. Security assessment questionnaires will be completed no more than once annually and may require reimbursement of the time expended by Diligent personnel, depending on the complexity and length of the questionnaire.

8. Security Controls Audit

Diligent has and will maintain a current SOC 2 Type II report (or industry-accepted successor security audit) prepared by a third party auditor consisting of a comprehensive internal controls assessment covering the internal controls and information security related to the Diligent Service. Upon request, Diligent will provide a copy of its then-current SOC 2 report to Client. The report is Confidential Information of Diligent and is subject to the confidentiality provisions of the Agreement.