SECURITY ADDENDUM

This Security Addendum is agreed between Gearset and Customer pursuant to the terms of the Gearset Master Services Agreement (which together with any attachments or supplements thereof constitutes the "**Agreement**") under which Customer has agreed to procure and Gearset has agreed to provide certain Services (as defined in the Agreement). This is version v1202609 which is effective from September 15, 2026.

This Security Addendum sets out non-exhaustive details of the administrative, physical, and technical safeguards implemented and maintained by Gearset to protect the security, confidentiality and integrity of Customer Data, summarising the minimum security standards maintained by Gearset. These may be subject to technical progress and development and Gearset may update or modify them from time to time at its sole discretion and without notice to Customer, provided always that such updates and modifications do not result in the material decrease in or degradation of the overall functionality or security of the Software or the Services subscribed for by Customer.

1. Definitions

1.1. Capitalised terms used but not defined in this Security Addendum have the same meanings as set out in the Agreement.

1.2. For the purposes of this Security Addendum the following words and phrases shall have the following meanings:

"**Gearset Personnel**" means Gearset and its affiliate's officers, directors, employees, agents, contractors, and consultants who may have access to Customer Data.

"**Security Incident**" means a violation of Gearset's or its computer security policies that has or is reasonably expected to have a material impact on Gearset's Services and business operations, including but not limited to unplanned disruptions, denials of service attack, malware infection such as ransomware, or an outside cyber-attack intended to disrupt, disable or destroy Gearset's computing environment.

"**Security Breach**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, transmitted, stored or otherwise Processed by Gearset or its Sub-processors of which Gearset becomes aware.

2. Security Governance

2.1. **Protection of Customer Data.** Gearset has and will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as summarized in this document. Gearset will not materially decrease the overall security of the Services during any Subscription Period.

2.2. **Security Program**. Gearset has and will maintain a comprehensive information security program that is aligned with industry best practices and appropriate to the nature and scope of Gearset's activities and services. This program utilizes a standard set of controls and includes the use of precautionary measures identifying internal and external risks and assessing the sufficiency of any systems and procedures in place to control these risks.

2.3. **Security Policies.** Gearset has and will maintain information security policies, standards and procedures, which shall be kept up to date, and revised whenever relevant changes are made that impact the security, confidentiality, and integrity of the Services provided. All policies are reviewed no less often than annually.

2.4. **Independent Attestation.** Gearset has and will continue to engage third party auditors to verify the adequacy of its security measures. These audits: (i) will be performed annually; (ii) will be performed according to internationally recognized standards; (iii) will be performed by independent third party security professionals at Gearset's selection and expense.

2.5. **Security Assessment Questionnaires.** Gearset shall grant Customer access to Gearset's Whistic profile, which contains up to date standard form security questionnaires. Not more than once per year, Gearset shall provide Customer with responses to reasonable questions from Customer, provided that the answers are not already available from within the Whistic profile.

2.6. **Certification.** Gearset has and will maintain certification to the ISO/IEC 27001 standard as external validation of its security controls. A copy of the certificate will be provided to Customer upon request.

2.7. **Other Reviews; Audits.** Gearset engages third party auditors to verify the adequacy of its security measures. These audits: (i) will be performed at least annually; (ii) will be performed according to internationally recognized standards; (iii) will be performed by independent third party security professionals at Gearset's selection and expense and (iv) will result in the generation of an audit report ("Audit Report") which will constitute Gearset's Confidential Information. No more than once during any consecutive 12-month period, on the Customer's written request and subject to the confidentiality obligations in the Agreement, Gearset shall make available to a Customer that is not a competitor of Gearset (or Customer's independent, third-party auditor that is not a competitor of Gearset) a copy of Gearset's then most recent Audit Report or the summary results, as appropriate. Within such request, the Customer shall be entitled to ask reasonable questions of Gearset related to its compliance with the terms of this agreement, and Gearset shall use its reasonable endeavors to respond adequately when providing the Audit Report.

2.8. **Security Contact**. In the event that Customer identifies a security issue or concern with Gearset, they can contact the appropriate personnel via security@gearset.com.

2.9. **Privacy Contact**. In the event that Customer identifies a data privacy issue or concern with Gearset, they can contact the appropriate personnel via privacy@gearset.com.

3. Personnel Management

3.1. **Background Checks.** Gearset will, in accordance with applicable law and regulation, perform, or require to have performed, criminal background checks for all Gearset Personnel with access to Customer Data prior to granting access to such data.

3.2. **Personnel security and nondisclosure**. All Gearset personnel with access to Customer Data shall be bound by obligations of confidentiality no less onerous than those set out in clause 7 of the Agreement.

3.3. **Security & Privacy Training.** Gearset has and will maintain a security and privacy awareness program to train all Gearset Personnel. This program will include but is not limited to training about: (i) data classification and handling; (ii) physical security controls; (iii) data protection; (iv) malware and phishing; (v) removable media; (vi) credential management, and; (vii) security incident reporting. Gearset provides such training upon hire and annually thereafter.

3.4. **Disciplinary Action.** Gearset has and will maintain policies to address Gearset Personnel violations of internal policies and procedures, and implement any disciplinary measures appropriate for the violation committed, including and up to termination of employment.

4. Access Management

4.1. **Physical Security**. Gearset has and will maintain appropriate physical security controls to prevent unauthorized physical access to areas in which Customer Data is handled, processed, or stored, over which Gearset has control.

4.2. **Hosting Infrastructure Security.** Gearset will ensure that all instances are hosted on Amazon Web Services ("**AWS**"). These AWS data centers offer state-of-the art physical and environmental protection for the servers and infrastructure that comprise Gearset's hosting environment.

4.3. **Access Controls**. Gearset has and will maintain commercially reasonable and appropriate technical controls, which shall follow industry best practices such as least privilege principle and segregation of duties, to prevent unauthorized access and disclosure of Customer Data.

4.3.1. Gearset will only grant Gearset Personnel access to systems that process or store Customer Data if it is required to perform their roles.

4.3.2. Gearset will no less than annually perform access reviews for all Gearset Personnel in accordance with its internal policy. Findings shall be remediated in a timely manner.

4.3.3. Gearset Personnel credentials will be promptly deactivated upon the termination of employment or the end of the relevant services being provided.

4.4. **Multi-Factor Authentication ("MFA")**. MFA will be used for all accounts to applications that store or process Customer Data. Where possible, Gearset will utilize hardware keys and will not utilize SMS as the

authentication method.

4.5. **Password Management**. Gearset has and will maintain password policies and controls to ensure that Gearset Personnel use strong (at least 16 characters), unique passwords for all services. Passwords will be stored in secured password vaults protected by MFA. Passwords will be rotated in the event of, or suspicion of, their compromise.

4.6. **Third-Party Management.** Gearset has and will maintain a third-party risk management program and ensure that all third-party service providers that have access to Customer Data employ technical and organizational security measures that meet Gearset's expectations and provide adequate protection to Customer Data.

5. Business Continuity and Disaster Recovery

5.1. Gearset has and will maintain a formal Business Continuity Plan ("**BCP**") and a Disaster Recovery Plan ("**DRP**") that clearly define roles and responsibilities of the applicable Gearset Personnel as well as set out the appropriate scope and purpose of contingency plans to ensure organizational resiliency.

5.2. The BCP and DRP will cover resiliency of both the organization itself and the Services.

5.3. The BCP and DRP will be tested annually, and associated findings resulting from plan testing must be remediated in a timely manner.

5.4. The BCP and DRP will be reviewed annually and updated as necessary to address new risks and align with industry standards.

6. Data Security and Management

6.1. **Data Availability**. Gearset will ensure that Customer Data is protected against accidental destruction or loss in line with our published RPO of 24 hours and RTO of 1 hour. Gearset will use reasonable commercial efforts to make the Software available 24 hours a day, 7 days a week, except for (i) scheduled maintenance (of which Gearset shall endeavour to give advance electronic warning), and (ii) any unavailability (including unplanned maintenance) caused by circumstances beyond Gearset's reasonable control.

6.2. **Data Loss Prevention**. Gearset has and will maintain controls to protect Customer Data from being shared or leaked via network file sharing, and which prevents the use of removable storage media (i.e. USB, CD, DVD etc.) on its endpoints.

6.3. **Data Return and Destruction**. Customer has the ability through its use of the Software to retrieve or delete Customer Data during the Subscription Period. On request, within 60 days of termination or expiry of the Agreement, Gearset will, at Customer's election, delete or return to Customer all relevant Customer Data (including copies) in Gearset's possession, save to the extent that Gearset is required by any applicable law to retain some or all of the Customer Data.

6.4. **Deletion Standard.** All Customer Data deleted by Gearset will be securely deleted using an industry-accepted practice designed to prevent data from being recovered using standard disk and file recovery utilities (e.g. secure overwriting, degaussing of magnetic media in an electromagnetic flux field of 5000+ GER, shredding, or mechanical disintegration).

6.5. **Data Residency.** Customer Data is processed and (where applicable) stored in Amazon Web Services data centres in specific hosting regions, selected by Customer when creating their account in the Software. Unless Customer has given written prior approval, Gearset will ensure that Customer Data will not be transferred out of the region selected by Customer.

6.6. **Encryption**. Gearset will ensure that Customer Data is encrypted to protect it against unauthorized access.

6.6.1. **Encryption at Rest**. Customer Data stored on Gearset managed or controlled systems, networks, and environments will be encrypted using industry standard mechanisms and cipher suites (such as AES-256).

6.6.2. **Encryption in Transit**. Customer Data that is transmitted between the Gearset Software and Third-Party Services shall be encrypted using industry standard mechanisms and cipher suites (such as TLS 1.2).

6.6.3. **Key Management**. Gearset utilizes dedicated encryption keys to encrypt Customer Data. Such encryption keys are uniquely associated with each Customer.

6.6.3.1. All keys are protected against modification; secret and private keys are protected against unauthorized disclosure.

6.6.3.2. When a cryptographic key is compromised, all use of the key will cease.

6.6.3.3. Encryption key management systems are designed so that the compromise of a single key does not cause failure to the wider Software.

7. Software Security

7.1. **Secure Software Development Life Cycle ("SDLC").** Gearset has and will maintain processes to promote SDLC practices to ensure the security, hygiene, and integrity of its code output. This includes regular code review, quality assurance checks, and adherence to applicable industry standards for coding practices.

7.2. **Production Environments**. Production environments will be logically and/or physically separated from any testing, development, or staging environments. Production code will not be released without Gearset Personnel first conducting code reviews and analysis.

8. Change Management

8.1. **Configuration and Change Management Policies.** Gearset has and will maintain formal configuration and change management policies which shall be reviewed and updated as needed, but in no case reviewed less than annually.

8.2. **Software Changes.** Any change to the Software will be documented in accordance with these policies, and will be implemented utilizing segregation of duties – the change performer must differ from the change approver.

9. Risk Management

9.1. Gearset has and will maintain a defined security risk management and assessment methodology to identify ongoing security risks and how to address them. Risk assessments will be reviewed at least annually, and whenever there is a significant change to company operations or products. Such risk assessments, their findings, and attendant remediation plans will be documented.

10. Asset Management

10.1. **Asset Management Program.** Gearset has and will maintain an asset management program which includes an inventory of all devices that connect to Gearset systems. Gearset will programmatically monitor and protect these devices, and ensure they are securely configured.

10.2. **Endpoint Protection**. Gearset has and will maintain the following controls for all devices that connect to Gearset systems:

10.2.1. ensure endpoints are encrypted (i.e. full disk encryption).

10.2.2. ensure a firewall is enabled on endpoints (where it is possible to do so).

10.2.3. ensure endpoints deploy an industry-standard anti-malware and anti-virus system which is centrally managed and performs regular scans.

10.2.4. ensure Gearset Personnel are utilizing the latest and most secure web- browser when accessing Gearset's production environment.

10.2.5. limit the administrative privileges of assets to only authorized Gearset Personnel with a need for access.

10.2.6. apply Operating System and server hardening controls to minimize the attack surface and protect

against malicious attacks.

10.2.7. configure endpoints to automatically apply critical Operating System patches.

11. Network Security

11.1. **Network Security.** Gearset secures its networks using a defence-in-depth approach that incorporates both commercially available equipment and industry standard techniques.

11.1.1. Gearset has and will maintain either a network or host-based Intrusion Detection Solution or Intrusion Protection Solution on all Gearset-controlled networks used to store, process, transmit or access Customer Data. These systems provide continuous monitoring of Gearset's network and early detection of potential security threats.

11.1.2. Unauthorized attempts to access the Gearset network will be investigated accordingly.

11.1.3. Gearset will collect, manage, retain, and analyse audit logs of events to help detect, investigate, and recover from unauthorized activity that may affect Customer Data. Logs will be kept and maintained for at least 12 months. If Gearset is providing any software (either as a service or as packaged software), Gearset will provide Customer access to an Audit and Reporting API at https://gearset.com/api/. Gearset will implement reasonable controls to control access to and prevent modification of security audit logs.

11.1.4. Gearset will review access logs regularly to ensure that access permissions are appropriate and necessary and to analyse them for security threats.

11.2. **Guest Access.** Gearset has and will maintain appropriate controls to ensure that only authorized devices are connected to its networks. Gearset will ensure that guests or unauthorized endpoints do not have access to Gearset's systems and production networks.

12. Vulnerability Management

12.1. **Vulnerability Management Program.** Gearset has and will maintain a Vulnerability Management Program that adheres to industry best practices. At minimum, Gearset will conduct scans for known vulnerabilities on all externally facing systems, environments, and networks that are managed and/or controlled by Gearset.

12.2. **Penetration Testing**. At least annually, Gearset will engage a qualified independent third- party supplier to conduct a penetration test of Gearset's externally facing production systems, network, and environments and produce a written report of the findings. A copy of the recent penetration test report will be made available to Customer upon request.

12.3. **Patching and Remediation.** All vulnerabilities identified through the scans/testing performed by Gearset will be remediated in accordance with the following timelines (risk ratings of vulnerabilities shall be based on the Common Vulnerability Scoring System):

12.3.1. Urgent, critical, and high-risk vulnerabilities will be remediated with 30 days of discovery;

12.3.2. Medium-risk vulnerabilities will be remediated within 90 days of discovery;

12.3.3. Low-risk vulnerabilities or those which have no impact on Customer Data will be remediated at Gearset's discretion.

12.4. **Mitigating Controls.** Should Gearset be unable to remediate the vulnerabilities within the defined time frame, mitigating controls will be implemented.

12.5. **Bug-bounty**. Gearset has and will maintain a bug-bounty and crowdsourced penetration testing program to encourage responsible disclosure of any vulnerabilities. Reported vulnerabilities are triaged, prioritized, and remediated in a timely manner in line with the remediation timelines.

13. Incident and Breach Management

13.1. **Incident Response Plan.** Gearset has and will maintain formal incident response policies and procedures ("**Incident Response Plan**" or "**IRP**") that respond to both Security Incidents and Security Breaches. The

IRP establishes responsibilities for incident oversight and management, and is reviewed at least annually to ensure its consistency with industry standards and company practices. Gearset trains all Gearset Personnel on IRP procedures.

13.2. **Breach Notification.** Gearset will notify Customer promptly, and in any case within 72 hours, after becoming aware of any Security Breach by emailing a customer appointed contact and providing incident detail, impact and a dedicated point of contact within Gearset that will engage with the Customer security team until the incident is remediated and information requested by Customer security is made available. Gearset shall make reasonable efforts to identify the cause of any Security Breach and take those steps as Gearset deems necessary and reasonable to remediate the cause of such a Security Breach to the extent the remediation is within Gearset's reasonable control. Gearset will provide reasonable updates to Customer regarding its investigation, remediation and resolution timeframe of the issue.

13.3. The notice to be provided above shall detail, to the extent relevant and reasonably available to Gearset at the time:

- the date and time of the Security Breach;
- the cause of the Security Breach, if known;
- the categories and approximate number of records of Customer Data affected;
- the likely consequences of the Security Breach;
- the measures taken, or proposed to be taken, by Gearset to address and remediate the cause of the Security Breach; and
- the name and contact details of the person from whom more information can be obtained.

13.4. Gearset shall keep Customer reasonably updated of any material developments to its investigation, handling and remediation of the Security Breach, and Customer and Gearset shall reasonably co-operate to mitigate the risk to each party.

13.5. The obligations in paragraph 13 shall not apply to incidents that are caused by Customer or its Authorised Users, or by access to the Services in breach of clause 4 (*Use of Services and Documentation, Customer Obligations*) of the MSA, unless and until the Customer has notified Gearset that they constitute a Security Breach in which case Gearset shall provide the Customer with reasonable assistance (at Customer's cost) in investigating the information set out in paragraph 13.3 above.

13.6. **Third-Party Notifications**. Gearset agrees that, except to the extent required by law, it shall not notify any third party (including any regulatory authority or customer) of any Security Breach without first obtaining Customer's prior written consent (which shall not be unreasonably withheld or delayed). Further, Gearset agrees that, subject to any legal obligation on Gearset, Customer shall have the sole right to determine: (i) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, or others; and (ii) the form and contents of such notice

14. Subcontracts

14.1. Should Gearset engage any subcontractors in relation to the provision of the Services, it shall enter into a written agreement with each subcontractor containing obligations relating to the security and confidentiality of data which are no less protective than those in the Agreement, to the extent applicable to the nature of the services provided by such subcontractor. Gearset shall be liable for the acts and omissions of its subcontractors to the same extent Gearset would be liable if performing the services of each subcontractor directly under the terms of the Agreement, except as otherwise set forth in the agreement.

15. Artificial Intelligence

15.1. Gearset shall not use, nor permit any third party to use, Customer Data to train any artificial intelligence or machine learning engine or system, neural network, or similar system except as expressly permitted by Customer in writing (such written consent may be withheld by Customer in its sole discretion).

16. HIPAA (if applicable)

16.1. **HIPAA Compliance**. If Customer has (a) executed a Business Associate Agreement ("**BAA**") with Gearset, and (b) Customer is using Gearset's HIPAA instances to process ePHI, and (c) Customer has followed Gearset's HIPAA implementation guidelines; then Gearset affirms that it has and will maintain appropriate safeguards for the ePHI as required by HIPAA, in accordance with the terms of the BAA.

17. Code Reviews

17.1. To the extent that Customer is using Gearset's Code Reviews licenses, Customer Data shall be processed and (where applicable) stored in AWS data centres in region AWS EU-West-1 (Dublin, Ireland). This is regardless of the Gearset hosting region chosen for use with other Gearset products.