INNERGY SECURITY EXHIBIT

Version Date: July 1, 2026

This Security Exhibit forms part of the Agreement between INNERGY and Customer and describes INNERGY's security practices for the Platform and related Services. Capitalized terms used but not defined in this Security Exhibit have the meanings given to them in the Agreement.

1. Security Program

INNERGY maintains administrative, technical, and organizational safeguards designed to protect the confidentiality, integrity, and availability of Customer Data, taking into account the nature of the Platform, the sensitivity of Customer Data processed through the Platform, and INNERGY's role as a cloud-based software provider.

INNERGY may modify or update its security practices, controls, tools, vendors, infrastructure, and processes from time to time, provided such modifications are designed to maintain or improve the overall level of protection provided for Customer Data.

2. Hosting Environment

INNERGY currently hosts the primary Platform environment on Microsoft Azure, with backup and recovery capabilities maintained through additional Azure regions and separate backup infrastructure. INNERGY may update its hosting architecture, cloud regions, or infrastructure providers from time to time, provided that such changes are designed to maintain the overall level of protection for Customer Data described in this Security Exhibit.

INNERGY relies on the applicable cloud provider's physical, environmental, network, and infrastructure security controls for the cloud infrastructure used to host the Platform.

3. Encryption

INNERGY uses encryption controls designed to protect Customer Data in transit and at rest.

Connections between Customer users and the Platform are encrypted using industry-standard secure transport protocols.

4. Access Controls

INNERGY maintains role-based access controls, network access-control measures, and privileged access management practices designed to limit access to Customer Data to authorized personnel with a business need, including least-privilege access practices, multi-factor authentication protections for applicable personnel access, and access removal or modification when access is no longer required.

5. Customer Account Security

The Platform includes safeguards designed to help Customer protect user accounts and manage access to Customer Data, including granular user permissions, two-factor authentication, password controls, bot and brute-force protections, and login audit logs.

Customer is responsible for managing its user accounts, configuring appropriate permissions and security features, and maintaining the confidentiality of user credentials.

6. Network and Application Security

INNERGY maintains technical safeguards designed to protect the Platform against unauthorized access and common application attacks, which may include web application firewall protections, cloud-provider security tools, endpoint protection, and virtual private network protections for applicable company system access.

7. Secure Development, Vulnerability Management, and Monitoring

INNERGY maintains software development, software quality assurance, vulnerability management, monitoring, and logging practices designed to reduce security and reliability risk for the Platform. These practices may include peer review, automated scans of third-party libraries and relevant software components, pre-release testing and other quality assurance processes designed to identify defects before release, monitoring for suspicious activity, escalation of security alerts, and logs reasonably necessary to support security monitoring, troubleshooting, and investigation.

8. Backups, Recovery, and Business Continuity

INNERGY maintains backup, recovery, and business continuity processes designed to support the availability and recoverability of Customer Data and Platform functionality following a service disruption, infrastructure failure, or other adverse event. Unless expressly stated in a separate service level agreement, INNERGY does not commit to a specific recovery time objective, recovery point objective, uptime commitment, service credit, or other service level under this Security Exhibit.

Customer databases are backed up on a regular basis, generally multiple times per day, and point-in-time database backups are generally retained for approximately 35 days. Non-point-in-time backups are currently maintained for approximately 6 months, subject to technical feasibility and INNERGY's then-current backup retention practices.

INNERGY maintains point-in-time database recovery capabilities for recent backup periods and may maintain additional off-platform backup copies.

Customer files and attachments are replicated across cloud regions, and deleted or overwritten attachments may be recoverable subject to technical feasibility and INNERGY's backup retention practices.

9. Personnel and Physical Security

INNERGY maintains personnel security practices designed to reduce security risk associated with employee and contractor access to company systems, including access based on job responsibilities and business need, security guidance and operational expectations for applicable personnel, security awareness training and simulated phishing for applicable personnel, and multi-factor authentication protections for applicable employee access.

INNERGY's Platform is hosted in Microsoft Azure data centers, and INNERGY relies on the applicable cloud provider's physical and environmental security controls for those facilities. For INNERGY office locations, INNERGY maintains physical security measures appropriate to the location.

10. Security Incidents

A "Security Incident" has the meaning given to it in the Agreement.

Upon confirming a Security Incident, INNERGY will notify Customer in accordance with the Agreement and provide information reasonably available to INNERGY about the Security Incident and mitigation steps taken or planned.

INNERGY's notification of or response to a Security Incident is not an admission of fault or liability.

Customer must promptly notify INNERGY of any suspected compromise of Customer user credentials, Customer systems, or Customer-managed accounts.

11. Third-Party Providers

INNERGY may use third-party service providers, subprocessors, and infrastructure providers to provide, support, secure, and improve the Platform. INNERGY remains responsible for its obligations under the Agreement when using such providers.

Third-party processing of Customer Personal Data is governed by the applicable data processing terms between the parties.

12. Security Documentation, Questionnaires, and Audits

Upon Customer's reasonable written request, and no more than once in any 12-month period unless required due to a confirmed Security Incident, INNERGY may provide then-current reasonable security documentation or respond to a reasonable security questionnaire regarding the Platform.

Any non-public security information provided by INNERGY is INNERGY Confidential Information and may be used solely to assess INNERGY's security practices in connection with the Agreement.

INNERGY is not required to disclose information that would compromise security, reveal third-party confidential information, violate law or contractual obligations, or expose sensitive internal security details.

Any audit, review, penetration test, vulnerability scan, or technical assessment of the Platform requires INNERGY's prior written approval, mutually agreed scope and timing, and must not interfere with INNERGY's operations, systems, customers, or security.

Customer is responsible for its own costs and any reasonable INNERGY costs incurred in supporting an approved audit or assessment beyond standard security documentation or questionnaire responses.

Customer may not conduct, or permit any third party to conduct, penetration testing, vulnerability scanning, load testing, automated security testing, scraping, denial-of-service testing, or similar testing of the Platform without INNERGY's prior written approval.

13. Customer Responsibilities

Customer is responsible for managing Customer user accounts, credentials, access permissions, security-feature configuration, systems, networks, browsers, devices, and integrations used to access the Platform. Customer is also responsible for promptly notifying INNERGY of suspected unauthorized access to Customer accounts or Customer Data and for using the Platform in accordance with the Agreement and applicable law.

14. Limitations

This Security Exhibit describes INNERGY's security practices for the Platform and does not modify any limitation of liability, disclaimer, indemnity, data processing term, service level term, or other risk allocation provision in the Agreement unless expressly stated otherwise.

INNERGY does not represent that the Platform is SOC 2 certified and is not required to obtain any certification, audit, assessment, or attestation unless expressly stated in the Agreement.

15. Order of Precedence

If this Security Exhibit conflicts with the Agreement, the Agreement controls, except to the extent this Security Exhibit expressly states that it supersedes a specific provision of the Agreement. If this Security Exhibit conflicts with a fully executed Data Processing Addendum between the parties, the Data Processing Addendum controls solely with respect to the processing of personal data.