ECOLAB DATA SECURITY ADDENDUM

This Ecolab Data Security Addendum ("Security Addendum") outlines the physical, technical and organizational measures that Ecolab uses for certain Ecolab cloud-based online programs ("Programs") in order to protect Customer Data stored in Program production environments. Ecolab may update this Security Addendum from time to time effective when posted.

Capitalized terms used but not defined in this Security Addendum have the meanings as set forth in the Ecolab Program Terms and Conditions or other written or electronic terms entered into by the parties governing Program subscriptions ("Program Terms").

1. Security Governance.

a. General. Ecolab maintains a written information security program that includes policies, procedures and controls aligned to the NIST Cybersecurity Framework and industry-standard practices designed to protect Customer Data stored in Program production environments from unauthorized access and disclosure.

b. Maintenance and Compliance. Ecolab's information security program is led by its Chief Information Security Officer or equivalent executive, who is responsible for coordinating, managing and monitoring Ecolab's information security function, policies and procedures, including periodic assessments performed as a part of Ecolab's risk governance activities. Ecolab's information security program is reviewed and updated periodically to reflect changes in its technology and practices and applicable laws.

c. Policies. Ecolab's information security policies will be documented, reviewed and approved by management (including after material changes), and published and communicated to employees and contractors as Ecolab determines appropriate and applicable.

2. Certifications and Audits.

a. Ecolab Audits. Ecolab conducts annual audits of its information security controls and information technology as a part of its compliance with the Sarbanes-Oxley Act.

b. Certifications and Audits of Hosting Partners. Ecolab hosts Program production environments in the data centers of industry-recognized hosting partners that have SSAE 18 SOC 2 Type 2 attestations or have ISO 27001 certifications or successor or equivalent attestations or certifications. Hosting partners may make information about their security and privacy-related audits and certifications available directly through their websites.

3. Physical, Technical and Organizational Security Measures.

a. Physical Security. Ecolab restricts physical access to its facilities through one or more of the following: on-site security, areas requiring a badge to access and CCTV cameras.

b. Technical Security.

i. Access Management. Ecolab utilizes practices designed to limit access by its personnel to Program production systems that store Customer Data, including based on the principles of least-privilege and need-to-know, including: (i) authentication and authorization mechanisms; (ii) policies regarding passwords and the use of login credentials for accounts in Ecolab systems; (iii) automatic account logout after a period of time; (iv) access privileges limited by role and job requirements; (v) access revoked upon termination or the end of the job requiring such access; and (vi) periodic review of access entitlements by management.

ii. Firewalls. Ecolab uses firewall technology to protect Program production environments and the Customer Data stored therein to the extent each is accessible via the Internet. Managed firewall rules will be reviewed in accordance with Ecolab's then-current operating procedures.

iii. Malicious Code. Ecolab uses antivirus and antimalware software to identify and protect Program production environments from the introduction of viruses, malware and similar malicious code. Such software is updated on regular intervals.

iv. Vulnerability Management. Ecolab has formal practices designed to identify and remediate technical security vulnerabilities that Ecolab identifies in Program production environments and also monitors relevant vendor alerts and security advisories. Ecolab assesses and implements patches (including vendor patches) in accordance with its vulnerability management practices, including reviews and testing of patches prior to installing them in Ecolab production environments. Ecolab generally prioritizes identified vulnerabilities based on their severity and potential impact using criteria such as the Common Vulnerability Scoring System (CVSS).

v. Change Management. Ecolab follows a formal change management process to administer changes to Program production environments, including changes to its underlying software and systems. Each change is reviewed in a test environment before being deployed.

vi. Encryption. Ecolab utilizes encryption standards consistent with or exceeding NIST recommendations. Pursuant to such standards Ecolab encrypts Customer Data at rest within Program production environments using encryption with AES-256-bit encryption (or the equivalent or better) and only allows encrypted connections using transport layer security TLS 1.2 (or the equivalent or better) to online Program production environments for the transfer of Customer Data.

vii. Data Deletion. Ecolab uses an industry standard such as NIST 800-88 (or similar standard) for the deletion of Customer Data from media used by Ecolab to provide the Programs.

viii. Event Logs. Program production environment log activities are centrally collected and secured in an effort to prevent tampering and monitored for anomalies by Ecolab's information security team.

ix. Security Coding Practices. Ecolab develops software using secure application development practices aligned with industry standard policies and procedures such as the OWASP Top Ten or a substantially equivalent standard.

x. Separation of Content. Ecolab has implemented and administers controls to prevent one customer from gaining unauthorized access to the Customer Data of another, including maintaining logical separation of Customer Data between its customers in the Program.

c. Organizational Security.

i. Security Training. Ecolab requires its employees who have access to Program production environments that store Customer Data to undergo annual security training.

ii. Vendor Risk Management. Ecolab maintains a vendor management program and where Ecolab determines it is appropriate or necessary to do so, Ecolab reviews the practices of its vendors and requires them to have appropriate information security practices, including requiring its hosting providers to maintain security practices that are, at a minimum, aligned with SOC 2 standards.

iii. System Access. In addition to requiring its employees to adhere to official Ecolab policies, Ecolab requires individual user accounts for its employees along with multi-factor authentication for critical systems and system administrator access and use.

4. Contingency Planning and Incident Response.

a. Contingency Planning. Ecolab maintains and administers disaster recovery and business continuity plans that are designed to minimize the impact from certain events to the provision and support of Programs. Ecolab tests its disaster recovery and business continuity plans as a part of its periodic internal audits and security assessments.

b. Incident Response.

i. General. Ecolab promptly investigates security incidents upon discovery and, where it determines appropriate, conducts a response, remediation, recovery and post-event analysis.

ii. Breach Notification. To the extent permitted by applicable law, Ecolab will notify Customer in writing without undue delay but not later than seventy-two (72) hours after Ecolab confirms that a security incident has resulted in unauthorized access to or disclosure of Customer Data of the Customer stored in a Program production environment ("Security Breach"). Ecolab will send notifications of any Security Breach to the primary contact for Customer specified in the Order Form for its initial subscription to the Program or as may be designated by the Customer when setting up its Program account.

iii. Updates. Where reasonably possible, Ecolab will update Customer about the Security Breach with information regarding evaluation of the root cause, potential impact, remediation actions taken and actions planned to prevent a future similar event.

5. Testing and Monitoring. Ecolab engages independent third parties to perform periodic information security risk assessments (including annual penetration tests on the Programs) as a part of its risk governance program, with the objectives being to test and evaluate the effectiveness of Ecolab's security practices, to develop and implement measures to address and mitigate risk, and to evaluate new and evolving security technology and practices and to assess new and evolving security risks. Ecolab addresses identified vulnerabilities in accordance with its then-current operating procedures.

6. Limitations. Ecolab's security commitments apply only for Programs whose official Ecolab product documentation or contract terms and conditions incorporate this Security Addendum by reference. With respect to Programs for which this Security Addendum is applicable, notwithstanding anything to the contrary herein or in any of the other terms comprising the Agreement between the parties, Ecolab's obligations apply only for Customer Data stored in Program production environments. This Security Addendum does not apply with respect to any other information or data or to any information or data provided by Customer or an End User in violation of the Documentation, the Program Terms or other terms comprising the Agreement between the parties.

Last updated: May 30, 2025