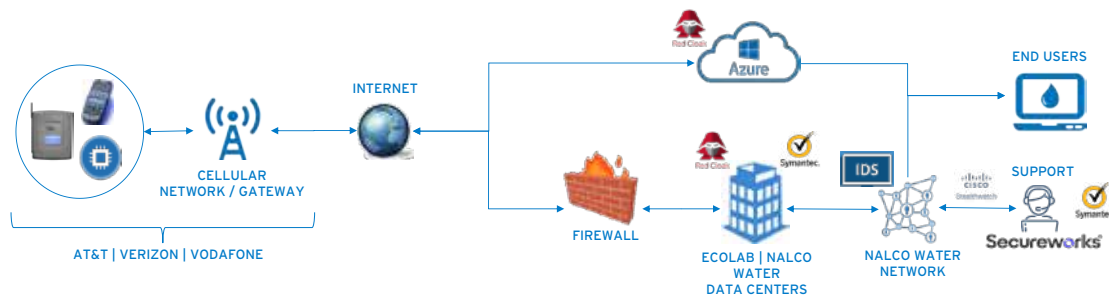# ECOLAB DATA MANAGEMENT POLICIES AND PROCEDURES

HOW WE PROTECT CUSTOMER DATA

Ensuring the security and integrity of our customers' data are top priorities for Ecolab. We follow National Institute of Standards and Technology cybersecurity framework standards in our data security governance approach. As a result, you can be assured that we are taking the utmost precautions, using state-of-the-art technology and trusted and established partners, to protect your information.

ECOLAB® | **NALCO** Water

Security Operations Center (SOC) Process Overview

Controls are an essential element of data security. Here are some of the ones that Ecolab has put in place to protect your information:

Governance for securing data

• Ecolab has established a **top-down approach** for policies and procedures. The Ecolab Security group reports directly to Ecolab's Chief Information Security Officer (CISO). The CISO chairs an executive-level steering committee that continually reviews IT security initiatives and oversees the governance of Ecolab's IT security programs.

• Ongoing initiatives include:
  - **Strategic security planning** with all Ecolab businesses from a risk-driven perspective
  - **Vendor risk-management** policies and programs, for cloud and service providers.
  - Mandatory company-wide annual **security awareness training** for all employees and contractors

Strong partnerships with Microsoft and other industry leaders

• We have engaged third-party, industry leaders for secure monitoring of network and cloud-based solutions.

• Ecolab works with Microsoft to build solutions on its Azure cloud computing platform, for most up to date compliance, visit http://www.microsoft.com/en-us/trust-center. This is the most comprehensive compliance coverage available, from the industry leader in customer advocacy and privacy.

• We also have partnerships with leading telecommunication companies to help manage secure data flow between customer-connected systems and our data centers.

Identity and access controls

Here are some additional ways that we protect access to your information:

• The **Microsoft Azure Active Directory** has been deployed to manage identities and create intelligence-driven access policies to secure all resources.

• **Customer access** is managed user-by-user through our portal, based on agreed-upon customer access policies communicated to the Ecolab sales team. Customers can only view data and insights. They do not have access to make remote controller changes.

• **Multi-factor authentication** is in place to prevent unauthorized access to critical systems, such as financial and human resources systems. This will expand to include other systems as security needs evolve.

• **Role-based access management** is used to control access to privileged accounts such as administrator-level accounts for both internal and customer accounts. In addition, our Human Resources systems automatically deny access to data and deauthorize personnel when they are out on extended leave, resign or are terminated.

Data transmission and storage

- Securing **data transmission and data** is a top priority for Ecolab for both in-transit data (actively moving across the internet or through a network) or inactive/at-rest data (stored in a device or network).

- Our on-premise critical solutions have been upgraded to meet today's high security standards for encrypted databases. We also have developed new solutions that can be implemented for in-transit data, to extend the life of older controllers.

- Our newer solutions leverage the Microsoft Azure cloud platform. Built with security from the ground up, these systems take advantage of Microsoft's robust protected environments, including **data encryption**.

Security incident response

- Ecolab has a **365/24/7 Security Operations Center** maintained by certified Security Service market leaders who engage with reputable third-party analytics and threat- intelligence providers to detect, prevent and alert us to any vulnerabilities or intrusion attempts.

- Through continuous monitoring and control of Ecolab network on-premise and cloud resources, we establish incident response procedures and staff appropriately for **advanced threat monitoring, response and resolution**.

Data backup and disaster recovery controls

- Ecolab has formal policies to ensure that **backups for all critical systems** are tested and maintained, and that backup media is secured and available for use in an emergency.

- **The Information Security Steering Committee (ISSC) and Ecolab management** review these controls and **ensure compliance** annually – at a minimum – for both on-premise systems (such as enVision) and cloud-based systems (such as Azure).

Risk management and audits

- Ecolab develops, disseminates and periodically reviews formal, documented **information security policies**, including risk management.

- Other policies include: **security awareness, security training, incident response, and identity and access management**. Formal, documented procedures facilitate the implementation of Ecolab's policies and associated **risk assessment controls**.

- Ecolab conducts annual **third-party penetration testing** and **security program reviews**.

Additional Information

No one document can answer every question about data security. If you would like more information about Ecolab's systems and how we protect your information, we are happy to speak with your staff or IT personnel. Your Ecolab Nalco Water representative can facilitate that discussion with our team or you can submit a request at www. ecolab.com/pages/security. We will then make arrangements to provide you with the answers that you need.