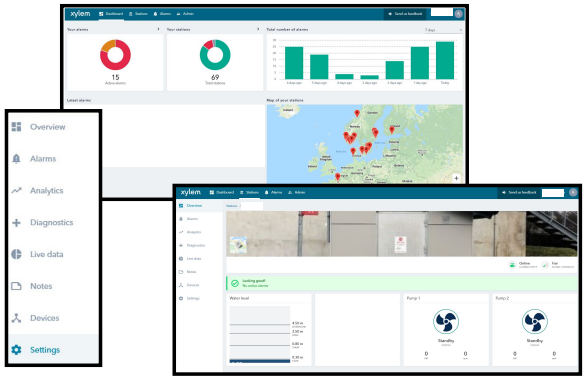
PRIVACY AND SECURITY POLICY

90027101_2.0



Avensor™

1 Cybersecurity at Xylem

Product cybersecurity is now a market imperative to gain the trust of our customers. Xylem recognizes this imperative, and aims to increase the faith and trust that our customers have in our products and services. Our customers clearly express their concerns about the safety of an increasingly cross-connected and cloud-based solution set. The Xylem cybersecurity team can help our customers' IT departments to maximize the capability of analytical and performance management. The most rigorous safety standards are adhered to, throughout the process.

2 Privacy protection

Xylem follows an internal privacy policy that includes the elements of the European Union (EU) General Data Protection Regulation (GDPR). Similar to the GDPR, the Xylem privacy policy is intended to help our customers to understand these items:

- What data that Xylem collects
- The way that Xylem uses the data
- The security that Xylem uses to protect the data
- The rights as allowed by applicable law

For more information about the privacy policy, see *More information* on page 2.

3 Data security

Xylem prioritizes the availability, integrity, and confidentiality of all the capabilities that we provide to our customers. The security of these products and services is governed by the Xylem product cybersecurity program.

4 The Xylem product cybersecurity program

Our mission is to bring innovation and industry best services to the global water industry. Therefore, Xylem has developed a product security program that is aligned to the industry and to the Three Lines of Defense model.

First line of defense

Each business unit in Xylem has a dedicated product security team that supports the related product lines. These teams have these functions:

- Builds the security of the products
- Responds to vulnerabilities and incidents
- Partners with customers to provide high levels of assurance

These teams are also scaled to reflect the size of each individual product portfolio.

Second line of defense

The global product security team has these functions:

- Monitors the risks across the Xylem product portfolio
- Serves as an escalation point for issues
- Represents the unified voice of Xylem about product security

This global team provides several services that are led by experts in the corporate team and largely fulfilled by commercial security partners. This organization creates scale for the individual business units. These services are key:

- The product security incident response team monitors vulnerabilities in the industrial space and our supply chain. They are ready to support customers with cybersecurity incidents that involve our products.
- The shared service capabilities ensure that the technology platforms include software security and align with new regulations in the industry.

Providing these services allows the product security teams to focus on what they do best – being product experts and consultative partners with engineering.

Third line of defense

The internal audit team at Xylem regularly audits the business units to ensure the overall effectiveness of the program. The quality and effectiveness of the program is important to both the Xylem board of directors, and the internal cyber risk committee.

The cyber risk committee receives monthly metrics. These metrics show the continuous internal efforts to improve the security of Xylem products that are under development and those that are used in the field.

5 Avensor™

Avensor™ uses the Xylem cloud platform, a smart infrastructure that enables the processing, transformation, and analytics of sensor data. When Avensor™ is combined with the Xylem cloud platform, it aligns to the Xylem product security program. The program helps to enable each platform so that our customers can gather valuable insights and make data-driven decisions safely.

Deployment

Avensor™ and the Xylem cloud platform are deployed on Amazon Web Services (AWS), and run in data centers with high availability. This includes all data such as backups. The locations are continuously evaluated and aligned to the needs of our customers, together with applicable compliance requirements.

6 Access and control of data centers

Cloud security environment

Xylem supports the use of world-class cloud computing partners to drive scale and increase security protection. Together with AWS, we operate on a shared accountability model that enables all participants to focus on their strengths.

The shared responsibilities are divided in these ways:

- AWS is responsible for the security of the cloud, which includes the security of AWS data centers. For more information, see *More information* on page 2.
- Xylem is responsible for the security in the cloud. We use the methods and resources that AWS provides to ensure the secure setup of our applications and define the correct data access.

Related aspects include:

- Protection against network-layer Distributed Denial of Service (DDoS) attacks
- Web application firewall (WAF) to safeguard against application-layer threats
- Private networks to keep selected dataflows isolated from the public internet
- Remote management of services via Virtual Private Network (VPN)
- Multi-factor authentication (MFA) for cloud administration and role-based access control
- Industry-standard encryption of data in transit and data at rest, for example, TLS, VPN, and AES
- Continuous security logging and monitoring
- Multiple high availability (HA) service instances that are deployed across multiple zones

Product security

The software development life cycle (SDLC) includes activities that support secure and reliable product development.

Related aspects include:

- Security framework based on best practices, for example, Xylem policy and the IEC 62443 standard
- Threat modeling and risk profiling to identify security risks
- Architecture reviews that address identified risks, and design for security considerations
- Security awareness to support the development effort, for example, secure code techniques
- Automated and manual security test to check and identify security vulnerabilities
- Close collaboration with the product security team

7 More information

- For more information about the Xylem product cybersecurity program and to contact our security team, go toxylem.com/security.
- For more information about AWS security practices, go to https://aws.amazon.com/compliance/shared-responsibility-model/.
- For more information about the Xylem privacy policy, go to https://www.xylem.com/en-us/support/privacy/.

Xylem Water Solutions Global Services AB 556782-9253
361 80 Emmaboda
Sweden
Tel: +46-471-24 70 00
Fax: +46-471-24 74 01
http://tpi.xyleminc.com

90027101_2.0_en-US_2021-03_GSI_Avensor™

xylem
Let's Solve Water