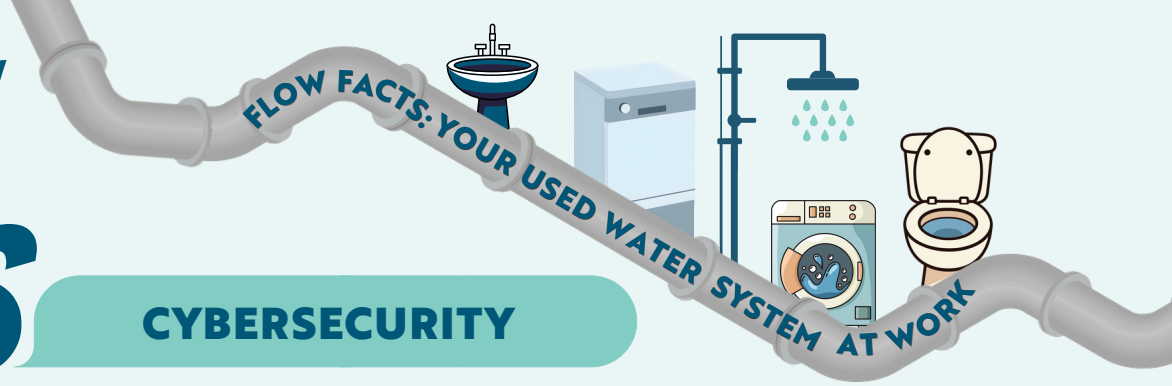
FLOW FACTS

CYBERSECURITY



Why does cybersucirity matter?

Cybersecurity is an organizational risk, not simply an IT issue. ARROW's technology environment supports both corporate business functions and critical wastewater operations. A significant cyber incident could affect operational continuity, financial systems, sensitive information, employee productivity, and ARROW's ability to deliver essential services.

What We Are Protecting?

ARROW's cybersecurity program is designed to protect **4** key areas:

People

Employees, contractors, and partners who access ARROW systems.

Information

Corporate records, financial information, and operational data.

Business Systems

Microsoft 365, financial & enterprise applications, servers, endpoints, and cloud services.

Operational Technology (OT)

Wastewater treatment, transmission and control systems

Primary cyber risks

ARROW operates in an environment where cyber threats continue to evolve. Key areas of risk include:

- Phishing and credential theft.
- Ransomware and malware.
- Unauthorized access from compromised accounts or systems.
- Third-party and supply-chain risk.
- Human error

Protecting our operations

Cybersecurity at ARROW extends beyond corporate IT to the Operational Technology (OT) systems that support wastewater treatment, transmission, monitoring and control. ARROW continues to strengthen OT security through improved monitoring, threat detection and specialized cybersecurity capabilities, while reducing risk through ongoing investment in technology, employee awareness, preparedness and business continuity.

ARROW continues to strengthen cybersecurity across both corporate IT and operational environments, with the goal of ensuring that a cyber event does not become a significant business or operational disruption.

How ARROW manages cyber risk

ARROW operates in an environment where cyber threats continue to evolve. Key areas of risk include:

1. **Prevent**
   Multi-factor authentication, access controls, endpoint protection, network security, system updates, security policies, and employee cybersecurity awareness.
2. **Detect**
   Continuous security monitoring, security technologies, logging and alerting, and enhanced monitoring of critical environments.
3. **Respond**
   Documented incident-response processes help ARROW identify, contain, investigate, and recover from cybersecurity events.
4. **Recover**
   Backups, infrastructure resilience, disaster-recovery planning, and business-continuity practices help ensure critical services can be restored following an incident.