



Document Title	ShieldNet Cybersecurity Standard Water and Wastewater Add-on
Release Date	December 2025
Next Review	December 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0
Version	1.0

1. What is the Water and Wastewater Add-on

Water and wastewater services are critical infrastructure sectors that face unique cyber threats. Municipal water utilities and sewer systems rely on industrial control systems (SCADA/ICS) to pump, treat, and distribute water- a compromise can disrupt essential public services or even threaten public health. Recent years have seen a rise in cyber-attacks on water utilities, from attempted water poisoning to ransomware on treatment plant networks. At the same time, new EU regulations have formally brought the water sector under stricter cybersecurity obligations: the NIS2 Directive (Directive (EU) 2022/2555) now includes drinking water supply and wastewater management as essential services, and the Critical Entities Resilience (CER) Directive (Directive (EU) 2022/2557) identifies water and wastewater among 11 key critical sectors. The ShieldNet Water and Wastewater Add-on extends the core 48 ShieldNet controls with additional safeguards tailored to this sector's needs. Each control is a concise "must-do" statement in plain English, geared toward small to medium organizations (municipal utilities, treatment plants, water contractors). By implementing these water-specific controls on top of the ShieldNet core, organizations can better protect water quality, ensure continuous supply and sanitation services, and meet regulatory requirements. The add-on maintains ShieldNet's practical tone- focusing on actionable steps and proportionate measures- to help resource-constrained teams secure vital water infrastructure without unnecessary complexity.

2. How to use the Water and Wastewater Add-on

Use this Water and Wastewater Add-on alongside the core ShieldNet controls, not as a standalone checklist. Water sector entities should first implement all relevant ShieldNet core controls (the baseline applicable to all sectors) and then augment them with the sector-specific controls from this add-on. Identify which category (or categories) below match your organization's role- e.g. a municipal drinking water utility would refer to Water Utilities, a wastewater treatment plant to Wastewater Operators, and an engineering firm servicing water infrastructure to Water Infrastructure Contractors. If one organization spans multiple roles (for instance, a combined water & sewer utility, or a utility that also has an internal engineering team), include all applicable controls from each relevant category. The add-on's structure mirrors the five ShieldNet Action Zones (Know & Plan, Shield & Build, Watch & Patch, React & Recover, Learn & Lift), making it easy to integrate these additional items into your existing security program framework.

ShieldNet uses a risk-based approach by organization size and sector criticality. The water sector is considered critical for societal well-being (clean water and sanitation are essential services). Thus, for any small or medium water-sector organization, these add-on controls should be treated as mandatory enhancements to the core controls. A very small (micro) utility or contractor should still implement as many add-on controls as feasible based on risk- at minimum those addressing legal obligations (e.g. incident reporting, basic ICS protections)- even if some advanced measures are scaled down due to limited capacity. Small and medium entities (up to ~250 staff) are expected to implement the full set of relevant add-on controls; medium-sized ones in particular should prepare for potential audits or oversight, as regulators under NIS2 will scrutinize cybersecurity for critical water and wastewater providers. In practice, adopting this add-on means updating your policies, procedures, and training to cover these water-specific requirements. For example, a water utility should update its incident response plan to include scenarios like SCADA sabotage or water contamination, and a contractor firm should build these controls into its project security plans and employee training. By following both the core and Water and Wastewater sector controls, even smaller organizations can achieve a level of security and resilience appropriate to the vital services they provide, while remaining practical and scaled to their resources.

3. Action Zones

All controls in this add-on are organized by ShieldNet’s five Action Zones, reflecting the security lifecycle. Water sector organizations should address all five zones for a comprehensive cybersecurity program:

- **KNOW & PLAN** - Understanding assets, risks, and compliance obligations in the water/sewer context, and planning accordingly.
- **SHIELD & BUILD** - Implementing protective measures and secure architectures tailored to water and wastewater operations (both IT and OT systems).
- **WATCH & PATCH** - Monitoring for threats or anomalies in networks and control systems, and keeping systems (including legacy ICS) up to date and hardened against vulnerabilities.
- **REACT & RECOVER** - Responding to incidents in a way that minimizes impact on public services (continuity of water supply, environmental protection) and recovering operations quickly.
- **LEARN & LIFT** - Learning from incidents and near-misses, improving continuously, and lifting the security maturity

Each control below is written in plain language and is directly actionable. We include references to EU directives and standards (like NIS2, CER, and other relevant regulations) to show alignment- adhering to these controls will help you meet those legal requirements. Use this add-on as a checklist or extension of your core ShieldNet implementation: integrate the controls into your risk assessments, update your incident response and continuity plans to cover these scenarios, and assign responsibility (e.g. IT/OT Security Coordinator, Plant Manager, Operations staff, etc.) for each control. Implement the Common Controls first- they form a baseline for all water sector entities and then layer on the Category Specific Controls that apply to your type of organization.



3.1. COMMON CONTROLS

The Common Controls are baseline cybersecurity requirements for all water and sewer organizations in ShieldNet (municipal water utilities, regional wastewater operators, water infrastructure contractors, etc.). They extend the Core Standard with water-specific safeguards (especially for industrial control systems and public service continuity) and are organized under the five Action Zones. Each control is proportionate for small teams, written in plain English, and mapped to EU sources where applicable (e.g. NIS2, CER Directive, Drinking Water safety provisions). Implement these common controls first. By doing so- and keeping records of policies, configurations, and training- you will establish an audit-ready foundation that protects critical water infrastructure, maintains service continuity, and supports compliance with the latest EU laws.

3.1.1. KNOW & PLAN

[KP-W1] Maintain Critical Asset Inventory

Control text: Identify and catalog all critical assets in your water/wastewater operations including SCADA/ICS components, treatment facility control systems, remote sensors/RTUs, and IT systems holding sensitive or operational data. Classify these assets by criticality (e.g. which systems' failure could disrupt water service or water quality) and apply security controls according to their sensitivity.

Why: You cannot protect what you do not know you have. A current inventory helps you focus security and monitoring on the systems that keep water services running.

Evidence examples: Asset inventory for IT and OT systems, criticality or classification ratings, network diagram showing key components, record of the last review date.

Legal anchors: NIS2 Art. 21(2)(a), CER Art. 11(2).

[KP-W2] Perform Cyber Risk Assessment

Control text: Perform a cybersecurity risk assessment focused on water and wastewater operations at least once a year and after major changes. Include realistic scenarios such as loss of SCADA visibility, ransomware on business systems, remote access abuse, or manipulation of treatment settings. Record the top risks and maintain a simple plan to reduce them.

Why: Risk assessments help you focus on what could disrupt water services. A simple plan turns findings into actions you can track.

Evidence examples: Risk assessment report, list of top risks with owners, action plan to reduce risks, review date and updates after major changes.

Legal anchors: CER Art. 6, CER Art. 11, NIS2 Art. 21(2)(b).

[KP-W3] Set Security Ownership and Contacts

Control text: Appoint one person to coordinate cybersecurity across both IT and control systems and give them authority to drive improvements. If you are an essential or important entity, nominate an official point of contact for authorities and the CSIRT and keep contact details up to date. Brief management regularly on key risks, incidents, and progress so accountability is clear.

Why: Clear ownership prevents gaps and delays when issues appear. A named contact also supports coordination with operators, suppliers, and authorities.

Evidence examples: Role assignment or job description, simple responsibilities matrix, meeting notes on security decisions, contact list for key partners and authorities.

Legal anchors: CER Art. 11(3), NIS2 Art. 21(1), NIS2 Art. 21(2)(f).

3.1.2. SHIELD & BUILD

[SB-W1] Segment Networks for Control Systems

Control text: Separate the control network from office IT and from any network that is not needed for operations. Allow only the minimum necessary connections through controlled gateways or firewalls and document what is permitted. Keep controllers, SCADA servers, and water quality devices in isolated zones with no direct internet access.

Why: Segmentation limits how far an attacker can move between office IT and control systems. It reduces the chance that a business incident stops operations.

Evidence examples: Network diagram with zones, firewall rules or access lists, list of allowed connections, change approval records for network changes.

Legal anchors: NIS2 Art. 21(2)(c).

[SB-W2] Control Access and Use Strong Authentication

Control text: Allow access to SCADA and control systems only to named users with roles that match their job and give the minimum privileges needed. Require multi factor authentication for remote access and for administrator actions, including vendor support, and use a secure path such as a VPN and a jump host. Remove default and shared accounts and review access regularly.

Why: Strong access control reduces the risk of unauthorized changes to control systems. It also supports accountability by linking actions to named users.

Evidence examples: User access list for SCADA and OT, multi factor authentication settings, privileged access procedure, records of periodic access reviews.

Legal anchors: NIS2 Art. 21(2)(i), NIS2 Art. 21(2)(j).

[SB-W3] Harden Systems and Secure Configurations

Control text: Use a secure configuration baseline for SCADA servers, operator stations, engineering workstations, controllers, sensors, and network devices. Turn off what you do not need, close unused ports, and restrict removable media such as USB. Protect remote vendor access with VPN and approvals and keep it disabled when not in use.

Why: Secure configurations remove common weaknesses and reduce attacks. Standard baselines also make systems easier to maintain and audit.

Evidence examples: Hardening standard or build guide, configuration checklists, evidence of baseline settings applied, results of configuration reviews.

Legal anchors: NIS2 Art. 21(2)(e), CER Art. 12(2).

[SB-W4] Secure Procurement and Manage Suppliers

Control text: Add cybersecurity requirements to purchasing and contracts for control systems, sensors, software, and service providers. Require patch support, vulnerability notifications, secure remote access, and basic security documentation such as an SBOM when available. Keep a list of critical suppliers and check they meet your security expectations.

Why: Suppliers and equipment can introduce risks into your environment. Clear requirements reduce surprises during deployment and support.

Evidence examples: Security clauses in contracts, supplier assessment results, acceptance checklist for new systems, record of firmware and software update sources.

Legal anchors: NIS2 Art. 21(2)(d), NIS2 Art. 24.

3.1.3. WATCH & PATCH

[WP-W1] Monitor Networks Continuously

Control text: Monitor both IT and control networks so you can spot unusual activity early. Use control system aware monitoring where possible to alert on new devices, unexpected remote sessions, or changes to controller logic and setpoints. Make sure alerts reach a responsible person or your SOC and that there is a simple escalation procedure.

Why: Monitoring helps you spot problems early, before they affect service and safety. It also provides data to investigate incidents.

Evidence examples: Monitoring dashboard screenshots, alert rules and thresholds, review logs or tickets from alerts, documented response steps for key alerts.

Legal anchors: NIS2 Art. 21(2)(b), CER Annex I.

[WP-W2] Manage Vulnerabilities and Apply Updates

Control text: Keep an up to date record of versions for key IT and control assets and follow vendor and sector advisories. Prioritize vulnerabilities by risk and apply patches in a planned way, testing first when changes could affect operations. If you cannot patch quickly, use compensating controls and set a date for remediation.

Why: Known vulnerabilities are a common path for attacks. Regular patching and compensating controls reduce exposure.

Evidence examples: Vulnerability scan reports, patch schedule and records, list of exceptions with risk acceptance, maintenance window and change records.

Legal anchors: NIS2 Art. 21(2)(e), NIS2 Art. 21(2)(c).

[WP-W3] Keep Audit Logs and Review Anomalies

Control text: Enable audit logging on SCADA applications, gateways, remote access tools, identity systems, and other critical systems. Store logs securely and keep them long enough for investigations, then review them regularly or use automated alerts. Focus on events that could affect operations, such as failed logins, alarm overrides, and configuration or program changes.

Why: Logs help detect unusual activity and support investigations. Regular review increases the chance you catch issues quickly.

Evidence examples: Logging configuration for key systems, central log storage or retention settings, log review checklist, examples of anomalies recorded and handled.

Legal anchors: NIS2 Art. 21(2)(a)&(b), NIS2 Art. 21(2)(i).

3.1.4. REACT & RECOVER

[RR-W1] Prepare Incident Response Plan

Control text: Write an incident response plan for cyber events that can affect water and wastewater services, including malware in SCADA and suspicious water quality signals. Define roles, escalation paths, and who contacts authorities, suppliers, and local partners. Test the plan at least yearly and update it after exercises or incidents.

Why: A clear plan reduces confusion during a cyber incident. It helps restore service faster and meet reporting duties.

Evidence examples: Approved incident response plan, contact list and escalation steps, playbooks for common scenarios, records of the last test or exercise.

Legal anchors: NIS2 Art. 23.

[RR-W2] Back Up Data and Test Recovery

Control text: Back up critical operational systems and configurations, including SCADA servers, historian data, controller logic, and key IT systems. Store backups in a way that resists ransomware, such as offline or immutable storage, and protect them with encryption and access control. Test restores regularly so you know you can recover safely and in the right order.

Why: Backups protect you from ransomware and accidental loss. Tested restores are the only way to know you can recover.

Evidence examples: Backup configuration and scope, backup success reports, restore test results, proof of offline or offsite backups.

Legal anchors: NIS2 Art. 21(2)(c), CER Art. 13(1)(d).

[RR-W3] Plan Continuity and Manual Fallbacks

Control text: Prepare manual and fallback ways to run essential processes when digital controls are unavailable. Document what operators can do locally for pumps, valves, and dosing and keep paper procedures and key contact lists available. Train staff and exercise these scenarios, including how you would communicate with the public if needed.

Why: Fallback procedures keep essential operations running when systems fail. Practicing them reduces safety risks under pressure.

Evidence examples: Manual operation procedures, continuity plan for key services, training records for operators, drill or exercise reports.

Legal anchors: CER Art. 12(2), NIS2 Art. 21(2)(c).

3.1.5. LEARN & LIFT

[LL-W1] Staff Cybersecurity Training & Awareness

Control text: Provide regular cybersecurity training for staff and contractors who work with water and wastewater systems. Include practical signs of interference for operators and engineers and basic phishing and safe device use for office staff. Make reporting simple and reinforce it during onboarding and at least annually.

Why: People make decisions that can prevent or cause incidents. Simple training builds good habits and faster reporting.

Evidence examples: Training materials, attendance records, awareness messages or posters, phishing simulation results or follow up actions.

Legal anchors: NIS2 Art. 21(2)(g), NIS2 and Art. 20.

[LL-W2] Security Audits and Exercises

Control text: Check your water and wastewater security controls regularly through self-assessments and periodic technical reviews. Include tabletop exercises for realistic scenarios and practical tests such as restoring from backup and running manual fallbacks. Track findings to closure and ensure management reviews progress.

Why: Audits and exercises reveal gaps before real incidents. They also show progress over time.

Evidence examples: Audit plan or checklist, audit results and findings, exercise or tabletop report, action tracker with owners and dates.

Legal anchors: NIS2 Art. 21(2)(f), CER Art. 12, CER Art. 13

[LL-W3] Incident Debriefs and Lessons Learned

Control text: After incidents and serious near misses, hold a short review with both IT and operations. Document what happened, what worked, and what must change in controls, procedures, and training. Assign owners and due dates for improvements and verify that actions were completed.

Why: Post incident reviews help you fix root causes and prevent repeat problems. Tracking actions turns lessons into improvements.

Evidence examples: Lessons learned report, corrective action list, evidence of changes implemented, management review notes.

Legal anchors: NIS2 Art. 20(4), NIS2 Art. 21(2)(f).

3.2. CATEGORY-SPECIFIC CONTROLS

The following Category-Specific Controls provide additional requirements for particular roles in the water & sewers sector, recognizing that risks and operations can differ. Start with the Common Controls above, then apply only the category sections that match your organization. These add-on controls narrow down “how” to implement security in each environment- for instance, water utilities must secure treatment processes and customer trust; wastewater operators must prevent environmental hazards; contractors need to securely support their clients- while preserving the same actionable style and legal mapping of ShieldNet. Each category’s controls are organized by the five Action Zones (though listed together for brevity), ensuring they integrate seamlessly with the core framework.

3.2.1. WATER UTILITIES (DRINKING WATER PROVIDERS)

[KP-W4] Assess Water Quality and Safety Risks

Control text: Include cyber to safety scenarios in your water safety and risk assessments. Consider changes to chemical dosing, filtration and disinfection controls, and falsified sensor readings. Link each scenario to specific safeguards and response steps so safe water remains the priority..

Why: Cyber issues can lead to wrong setpoints, incorrect dosing, or loss of visibility. Including cyber in safety reviews helps protect consumers and operators.

Evidence examples: Safety or risk assessment including cyber scenarios, list of critical parameters and alarms, mitigation actions with owners, record of review and updates.

Legal anchors: Drinking Water Directive (EU) 2020/2184 Art. 8

[SB-W5] Implement Treatment Process Fail-safes

Control text: Implement independent safeguards that prevent unsafe treatment conditions even if SCADA is compromised. Use hardwired limits, interlocks, and local alarms that can stop or divert flow when thresholds are exceeded. Test these safeguards and maintain them like any other safety function.

Why: Fail safes reduce harm if controls are misused or unavailable. They help keep treatment processes within safe limits.

Evidence examples: Design documentation for interlocks and alarms, tested threshold settings, evidence of independent safety controls, maintenance test records.

Legal anchors: Drinking Water Directive (EU) 2020/2184 Annex II.

[RR-W4] Prepare Public Communication Plan

Control text: Prepare an external communication plan for cyber incidents that can affect service availability or water safety. Define triggers for public notices and pre approve simple messages for the main channels you will use. Coordinate with public health authorities and train a spokesperson.

Why: Clear communication maintains trust during disruptions and safety events. Prepared messages reduce delays and mistakes.

Evidence examples: Public communication plan, contact list for regulators and public channels, message templates, record of review or exercise.

Legal anchors: Drinking Water Directive (EU) 2020/2184 Art. 17, NIS2 Art. 7(5).

3.2.2. WASTEWATER OPERATORS

[KP-W5] Assess Environmental Impact Risks

Control text: Add cyber scenarios that could cause environmental harm or permit breaches to your risk assessment. Consider forced untreated discharge, manipulation of outflow controls, or tampering with effluent sensors. Record the highest risks and map them to preventive and emergency measures.

Why: Cyber incidents can cause spills, overflows, or illegal discharges. Assessing environmental impacts helps you prioritize protections and response steps.

Evidence examples: Environmental risk assessment including cyber triggers, list of high impact sites, mitigation plan and actions, coordination notes with relevant authorities.

Legal anchors: CER Annex I; Environmental Liability Directive 2004/35/EC.

[SB-W6] Protect Overflow and Spill Prevention Systems

Control text: Use physical and operational safeguards that reduce the chance of sewage overflow during failures or attacks. This can include secondary level sensors, automatic pump actions, backup power, and isolation gates. Maintain and test these protections regularly.

Why: Overflows and spills can harm people and the environment. Protecting and monitoring these systems reduces the chance of unnoticed releases.

Evidence examples: Inventory of overflow prevention systems, alarm and telemetry settings, inspection and maintenance logs, response procedure for overflow events.

Legal anchors: Urban Waste Water Treatment Directive 91/271/EEC, CER Art. 12(2).

[RR-W5] Prepare Emergency Treatment and Disposal

Control text: Document how you will keep treatment running if SCADA or automation is unavailable. Include manual procedures, use of storage basins and portable equipment, and coordination steps to reduce inflow if needed. Exercise the plan and keep mutual aid arrangements ready.

Why: Clear emergency procedures reduce harm when treatment is disrupted. They help staff act safely and consistently.

Evidence examples: Emergency treatment and disposal procedures, approval by management, training records, drill reports or incident logs.

Legal anchors: CER Art. 11(1), 12(2); Water Framework Directive 2000/60/EC.

3.2.3. WATER INFRASTRUCTURE CONTRACTORS

[KP-W6] Plan Security for Projects and Changes

Control text: For each major engagement, include a short cybersecurity plan that covers what systems you will access and how you will protect them. Agree with the client on remote access rules, change windows, and who to call if something goes wrong. Keep evidence that the client approved the security procedures.

Why: New projects often introduce new systems and access paths. Planning security early avoids costly fixes later.

Evidence examples: Project security checklist, design review notes, risk assessment for changes, go live approval records.

Legal anchors: NIS2 Art. 21(2)(d).

[SB-W7] Secure Remote Support Access

Control text: Use only client approved remote support methods with strong encryption and multi factor authentication. Keep access separated per client with unique accounts and log remote sessions, enabling access only when needed. Secure your support devices with patching, endpoint protection, disk encryption, and safe storage for configuration files.

Why: Remote support is useful but can be a high risk entry point. Secure tools and controls reduce the chance of misuse.

Evidence examples: Approved remote access method, multi factor authentication and session controls, vendor access agreement, access log review records.

Legal anchors: NIS2 Art. 21(2)(i).

[WP-W4] Protect Client Data and Confidentiality

Control text: Protect client information such as network diagrams, controller programs, credentials, and logs as confidential. Store it only in encrypted, access controlled repositories and share it using secure transfer methods. Delete or return the data when it is no longer needed and define retention in the contract.

Why: Customer and client data must be protected from misuse and leaks. Clear handling rules reduce privacy and reputation risks.

Evidence examples: Data handling procedure, access controls for customer data, encryption settings where used, records of data requests and responses.

Legal anchors: GDPR (EU) 2016/679 (processor safeguards for any personal data); contractual confidentiality; NIS2 Art. 24 .

3.2.4. BULK WATER & SHARED INFRASTRUCTURE OPERATORS

[KP-W7] Map Dependencies and Shared Service Risks

Control text: Map dependencies with other operators and shared services that could affect water or wastewater delivery. Identify technical and organizational single points of failure and agree escalation contacts across parties. Use this map in risk and continuity planning and review it when changes occur.

Why: Water services often rely on power, telecoms, and shared providers. Mapping dependencies helps you plan for outages and coordinated incidents.

Evidence examples: Dependency map, list of key suppliers and agreements, risk assessment for shared services, contingency plans for key dependencies.

Legal anchors: NIS2 Art. 21(2)(a),(c), CER Art. 12.

[RR-W6] Coordinate Restoration and Mutual Aid

Control text: Agree with partner entities how you will restore shared assets after a cyber incident. Define priorities, minimum service levels, and how you will isolate a compromised connection while keeping operations safe. Exercise the procedure together at least annually and improve it after the test.

Why: Restoration may depend on partners, shared assets, and mutual aid. Clear arrangements speed up recovery and reduce conflicts.

Evidence examples: Mutual aid agreements, restoration prioritization plan, contact list and call tree, records of joint exercises.

Legal anchors: NIS2 Art. 21(2)(c), CER Art. 11(1), CER Art. 12.

3.2.5. WATER QUALITY LABORATORIES & MONITORING SERVICE PROVIDERS

[WP-W5] Protect Integrity of Water Quality Data

Control text: Protect the integrity of water quality data so it cannot be changed without detection. Use authenticated collection where possible, keep audit trails for edits, and require a second review for critical parameters. Store raw data and final reports in tamper evident storage with reliable time stamps.

Why: Operational decisions rely on accurate water quality data. Integrity checks help prevent errors and detect tampering

Evidence examples: Controls for data entry and approvals, audit trails for lab and sensor results, calibration and validation records, exception reports for unusual results.

Legal anchors: NIS2 Art. 21(2)(a),(i), GDPR Art. 32.

[RR-W7] Escalate Abnormal Results and Suspected Tampering

Control text: Create a rapid escalation process for abnormal results or suspected compromise of water quality data. Notify the operator quickly, state whether the result is confirmed or suspected, and explain next steps. Preserve raw readings, logs, and analyst notes so an investigation can follow.

Why: Abnormal results may signal safety issues or data compromise. Fast escalation supports timely containment and public protection.

Evidence examples: Escalation procedure, thresholds and triggers list, example incident tickets, communication records for escalations.

Legal anchors: NIS2 Art. 21(2)(b).

3.2.6. WATER/WASTEWATER TECHNOLOGY PROVIDERS (OT/ICS VENDORS & INTEGRATORS)

[KP-W8] Document Essential Service Dependencies and Customer Impact

Control text: For each product or managed service used in water operations, document what essential function it supports and what security conditions you assume. Explain how customers should deploy it safely, including network separation, identity model, and remote access approach. Provide guidance on failure modes and safe fallback options.

Why: Documenting essential services and dependencies helps you focus on what must be protected first. It also supports clear decisions during incidents.

Evidence examples: Essential service statement, list of critical customer groups, prioritization criteria, management approval or review record.

Legal anchors: NIS2 Art. 21(2)(d), NIS2 Art. 21(2)(e).

[SB-W8] Use Secure by Default OT Configurations

Control text: Deliver products and reference deployments with secure default settings. Ensure default passwords are removed, roles are least privilege, logging is enabled, and management access uses encryption and safe remote access patterns. Where legacy limits exist, provide compensating controls and a short hardening checklist.

Why: Secure defaults reduce mistakes during deployment and upgrades. They also make your environment more consistent and easier to audit.

Evidence examples: Configuration baseline, deployment checklist, test results for default settings, change control records for deviations.

Legal anchors: NIS2 Art. 21(2)(e), CRA Annex I.

[SB-W9] Manage OT Software Components and SBOM

Control text: Maintain control over third party and open source components used in your OT software and firmware. Produce an SBOM for each release and protect the build and release process with signing and restricted access. Share SBOMs and component risk notes with customers or authorities when required.

Why: Knowing what software and components you run helps you respond to vulnerabilities quickly. It also supports supplier accountability.

Evidence examples: Software and component inventory, SBOM files from suppliers, version and patch tracking, policy for approving and updating components.

Legal anchors: NIS2 Art. 21(2)(d),(e).

[WP-W6] Set Coordinated Disclosure and Update Commitments

Control text: Run a coordinated vulnerability disclosure process with a clear reporting channel and defined response times. Provide advisories with mitigation steps and realistic patch timelines, including workarounds when patches are delayed. Notify affected water sector customers quickly and support them with indicators of compromise when relevant.

Why: Vulnerabilities may be found by customers, researchers, or vendors. A clear disclosure and update process ensures you receive fixes and apply them safely.

Evidence examples: Vulnerability disclosure policy, contact channel for reports, patch advisory process, records of disclosures and implemented fixes.

Legal anchors: NIS2 Art. 21(2)(e).

[RR-W8] Coordinate Incidents with Water Operators

Control text: Maintain an incident coordination process with customers for security events affecting deployed OT products or services. Provide a 24/7 escalation path for high severity issues

and help operators contain the problem, such as by disabling remote access and rotating credentials. Preserve relevant forensic data and provide safe recovery steps.

Why: Many incidents require coordination across operators, vendors, and authorities. Clear roles and information sharing reduce delays and duplication.

Evidence examples: Coordination procedure, contact list and escalation paths, shared incident log or ticketing record, notes from joint incident calls.

Legal anchors: NIS2 Art. 21(2)(b),(c).