



ShieldNet

Document Title	ShieldNet Cybersecurity Standard – District Heating & Cooling Add-on
Release Date	January 2026
Next Review	December 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0
Version	1.0

1. What is the District Heating & Cooling Add-on

The District Heating and Cooling Add-on is a sector focused extension to the ShieldNet Core Standard. The Core Standard provides the baseline cybersecurity controls that every SME should implement regardless of industry. This add on builds on that baseline and adds practical controls that reflect how district heating and cooling services actually operate, including operational technology, remote maintenance, field assets, customer connected interfaces, and the cyber physical safety aspects of temperature, pressure, flow, and service continuity. It is designed to be applied without increasing complexity beyond what an SME can sustain, while still raising assurance in the parts of the environment that are most exposed and most safety relevant.

This add-on is anchored in EU legal requirements that are particularly relevant for district heating and cooling. It uses NIS2 to translate cybersecurity risk management and incident handling expectations into sector specific measures, with emphasis on risk-based prioritization, access control, business continuity, monitoring, and secure supply chain practices. It uses the Critical Entities Resilience directive to reflect resilience expectations for essential services, especially planning for disruption, dependencies, and continuity during crisis conditions. It also incorporates product and data obligations where they commonly affect the sector, including the Cyber Resilience Act for connected products and vulnerability handling, the Radio Equipment framework for wireless connected devices, the Data Act for secure data access and sharing around connected product data, and GDPR where metering, customer portals, or operational data can constitute personal data. The purpose of referencing these acts is not to restate legislation, but to provide implementable controls that help organizations demonstrate alignment to concrete legal duties.

2. How to use the District Heating & Cooling Add-on

Use this add on as a second layer after you have implemented the ShieldNet Core Standard. The Core Standard establishes the minimum security foundation across governance, identity and access, asset management, backup and recovery, incident response, and basic monitoring. Once that foundation is in place, you apply the add on to address the additional exposure and impact that is specific to district heating and cooling operations. For smaller organizations with limited digital scope, the add on can be applied selectively to the most critical services and assets first. For organizations that meet NIS2 thresholds or are treated as critical under national implementation of CER, the add on should be treated as mandatory for the in scope parts of the environment, because it targets controls that directly support regulatory expectations for risk management, continuity, and incident readiness.

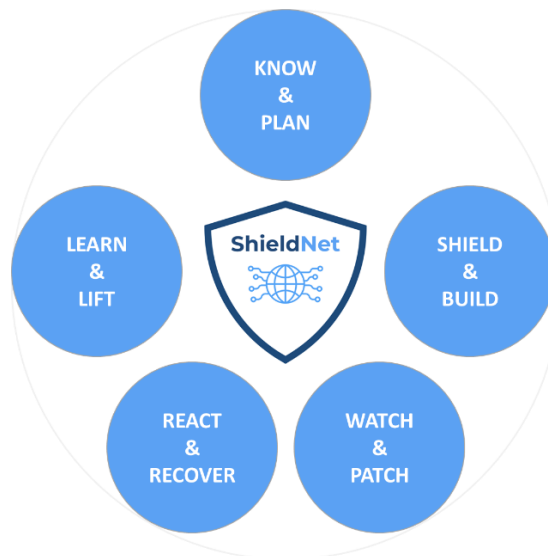
The add on is structured to be simple to apply. First, implement the common controls across all five Action Zones, because these reflect baseline sector risks that exist in almost every district heating and cooling organization, such as remote access pathways, separation between operational control and office IT, protection of controller configurations, and preparation for manual operation during disruption. Second, select detailed controls for your organization type, because different roles in the sector face different attack paths and responsibilities. For example, network operators will focus more on substation impact tiers and operational anomaly monitoring, building owners will focus on BMS integrations and sensor integrity, service providers will focus on platform tenant isolation and technician tooling, and manufacturers will focus on secure updates and vulnerability handling. This structure ensures that every organization applies the shared sector essentials, while only adding the additional controls that match its specific functions, scale, and criticality.

3. Action Zones

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

- **KNOW & PLAN** - Understanding assets, risks, and compliance obligations in the heating and cooling context, and planning accordingly.
- **SHIELD & BUILD** - Implementing protective measures and secure architecture tailored to district heating/cooling operations (covering both IT systems and operational technology in plants and networks).
- **WATCH & PATCH** - Monitoring for threats or anomalies in networks and control systems and keeping systems (including legacy ICS and smart controllers) up to date and hardened against vulnerabilities.
- **REACT & RECOVER** - Responding to incidents in a way that minimizes impact on heat/cooling delivery (continuity of service to households, businesses, critical facilities) and recovering operations quickly.
- **LEARN & LIFT** - Learning from incidents and near-misses, improving continuously, and lifting the security maturity of the organization over time.

Each control below is written in plain language and is directly actionable. We include references to EU directives and standards 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 for each control.



3.1. COMMON CONTROLS

The Common Controls are baseline cybersecurity requirements for all District Heating and Cooling organizations in ShieldNet.

3.1.1. *KNOW & PLAN*

[KP-HC1] Identify Thermal Service Criticality

Control text: List your essential heating or cooling services and link each one to the systems that control it such as plants substations building automation or customer portals. Mark which failures could cause safety risk service outage or major cost. Keep the list short and update it after major changes.

Why: Heating and cooling failures can become safety incidents quickly and cyber events often start in supporting systems. A clear criticality view prevents misaligned priorities.

Evidence examples: Service map, list of critical control points, approval by operations owner, change log.

Legal anchors: NIS2 Art. 21(2)(a), NIS2 Art. 21(2)(i), CER Art. 12(1).

[KP-HC2] Map Remote Access Paths for Operations and Maintenance

Control text: Remote access is the most common entry point in building and district heating incidents. Knowing the paths enables practical hardening and monitoring.

Why: Remote access is a common entry point in heating and cooling incidents. Knowing the paths enables practical hardening and monitoring.

Evidence examples: Remote access inventory, vendor access register, decommission records, review sign off.

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

[KP-HC3] Define Cyber Physical Safety Boundaries

Control text: Identify which setpoints commands and schedules can create unsafe conditions such as overheating freezing pressure excursions or loss of ventilation. Define acceptable ranges and who can change them. Require an operations owner to approve any change to these safety relevant parameters.

Why: In heating and cooling, cyber compromise can directly change physical conditions. Guardrails reduce the chance of unsafe or costly outcomes.

Evidence examples: List of safety relevant parameters, approval workflow, configured limits, audit trail of changes.

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

3.1.2. SHIELD & BUILD

[SB-HC1 Protect Controller Configuration Backups]

Control text: Store backups of PLC BMS and plant controller configurations in a secure repository with restricted access. Verify you can restore the configuration on a test device or a maintenance window at least yearly. Keep at least one offline copy.

Why: Configuration loss or malicious change is a primary recovery challenge in heating and cooling. Reliable backups shorten outages and prevent unsafe improvisation.

Evidence examples: Backup inventory, access list, restore test record, offline copy log.

Legal anchors: NIS2 Art. 21(2)(c), NIS2 Art. 21(2)(i), GDPR Art. 32(1)(c).

[SB-HC2] Harden Remote Maintenance Sessions

Control text: Require multi factor authentication for all remote maintenance to BMS and plant systems and use time limited access approvals. Record every remote session and the actions performed. Block generic shared accounts for maintenance.

Why: Vendor access is necessary, but it must be controlled to avoid persistent compromise. Session records enable investigation and accountability.

Evidence examples: MFA configuration, approval tickets, session logs, account list showing named users.

Legal anchors: NIS2 Art. 21(2)(j), NIS2 Art. 21(2)(i), CER Art. 13(1)(e).

[SB-HC3] Separate Building and Plant Control Networks from Office IT

Control text: Ensure BMS and plant control networks are isolated from office networks using gateways with explicit rules. Allow only the minimum required protocols and destinations. Review rules after any new integration or contractor onboarding.

Why: Heating and cooling controls are often compromised through office IT or unmanaged integrations. Segmentation reduces blast radius and supports monitoring.

Evidence examples: Network diagram, firewall rule set, change reviews, integration approval record.

Legal anchors: NIS2 Art. 21(2)(i), NIS2 Art. 21(2)(e), CER Art. 13(1)(b).

[SB-HC4] Embed Security Requirements into HVAC Procurement

Control text: For any new connected controllers gateways meters or optimization services require support duration update method and security contact details in procurement. Require evidence of vulnerability handling and secure defaults. Reject products that cannot meet basic requirements.

Why: Procurement is the cheapest time to reduce long term cyber cost in heating and cooling assets. Clear requirements improve supplier behavior without complex audits.

Evidence examples: Procurement clauses, supplier questionnaires, acceptance checklist, rejected product rationale.

Legal anchors: NIS2 Art. 21(2)(d), NIS2 Art. 21(2)(e), CRA Art. 13(5).

3.1.3. WATCH & PATCH

[WP-HC1] Detect Unauthorized Operational Changes

Control text: Monitor for changes to schedule setpoints and control logic on BMS and plant systems and alert on out of hours or unusual patterns. Include alerts for repeated failed logins and new remote connections. Route alerts to a named-on call role.

Why: Attackers often act by changing operational parameters rather than encrypting data. Early detection reduces physical impact.

Evidence examples: Alert rules, sample alerts, on call Rota, incident tickets created from alerts.

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

[WP-HC2] Centralize Logs for BMS and Plant Systems

Control text: Collect logs from gateways remote access systems operator workstations and key controllers when feasible. Keep logs tamper resistant and searchable. Review at least weekly or use automated correlation.

Why: SME environments often have limited visibility across mixed vendor systems. Central logs enable investigations and support vendor accountability.

Evidence examples: Logging architecture, retention settings, weekly review checklist, correlation rules.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 21(2)(f), GDPR Art. 32(1)(d).

3.1.4. REACT & RECOVER

[RR-HC1] Prepare Manual Operation and Safe Degradation Procedures

Control text: Document on how to continue safe heating or cooling service if automation fails including manual valve and pump operation and safe setpoints. Train operators and technicians on these procedures yearly. Store the procedures offline and in the control room where applicable.

Why: Heating and cooling systems must remain safe even during cyber disruption. Manual fallback reduces outage duration and safety risk.

Evidence examples: Manual operation guide, training records, offline copies, tabletop drill notes.

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

[RR-HC2] Define Incident Escalation for Service Continuity and Customer Impact

Control text: Define who declares an incident, who contacts vendors and who communicates to customers and local authorities when service is disrupted. This includes decision triggers based on safety and outage duration. Test the escalation at least yearly with a short scenario exercise.

Why: Heating outages can become public safety events and delays in communication increase harm. Clear escalation prevents confusion in SMEs.

Evidence examples: Escalation matrix, contact list, exercise report, updated procedures.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 21(2)(c), CER Art. 15(1).

3.1.5. LEARN & LIFT

[LL-HC1] Run Seasonal Cyber Readiness Reviews

Control text: Before each heating or peak cooling season review key risks remote access lists backup status and vendor readiness. Assign a short action list and track completion. Repeat a lighter review mid-season.

Why: Heating and cooling risk is seasonal, and SME capacity is limited. Seasonal reviews align effort with peak operational exposure.

Evidence examples: Seasonal checklist, action list, completion evidence, mid-season review note.

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

3.2. CATEGORY-SPECIFIC CONTROLS

The following Category-Specific Controls provides additional requirements for roles in the district heating and cooling 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, network operators must secure distribution networks and customer service continuity; plant operators must prioritize process safety and reliable heat production; building node service providers must securely support multiple client sites; and heating technology providers must build security into the products and services they deliver, 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. DISTRICT HEATING AND COOLING OPERATORS

[KP-HC4] Classify Substations and Field Nodes by Impact

Control text: Group substations and field nodes by impact on population served and by ability to isolate them operationally. Prioritize cyber controls for the highest impact groups first. Review the grouping before each heating season.

Why: District networks have many similar nodes and SMEs need a practical prioritization method. Impact grouping improves risk reduction per euro spent.

Evidence examples: Substation tiers, prioritization rationale, seasonal review record, action backlog.

Legal anchors: NIS2 Art. 21(2)(a), CER Art. 12(2), CER Art. 13(1)(a).

[SB-HC5] Implement Setpoint Change Control for Network Operations

Control text: Require a formal approval for changes to supply temperature curves pressure targets and pumping schedules that affect network stability. Use role-based access so only authorized operators can apply approved changes. Keep an audit trail of who changed what and when.

Why: Targeted setpoint changes can create widespread disruption without triggering traditional IT alarms. Change control prevents accidental or malicious instability.

Evidence examples: Change procedure, role definitions, audit logs, sample approved change records.

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

[WP-HC3] Monitor Network Anomalies as Cyber Signals

Control text: Define operational anomaly indicators such as unexpected temperature drops unexplained valve positions or pump behavior that deviates from weather and demand. Correlate these indicators with remote access and configuration change logs. Escalate anomalies that match cyber patterns to both operations and IT security.

Why: District networks provide strong physics-based signals that can reveal cyber manipulation. Correlation reduces false alarms and accelerates triage.

Evidence examples: Anomaly indicator list, correlation playbook, cross team escalation record, example investigations.

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

[RR-HC3] Coordinate Cyber Response with Operational Dispatch

Control text: Integrate cyber incident steps into dispatch operations so that network switching isolation and pressure management actions are pre planned. Define how to isolate compromised

substations while maintaining service to others. Run a joint drill with operations and IT at least once per heating season.

Why: District heating response requires coordinated operational decisions under time pressure. Joint drills reduce the risk of cascading failures.

Evidence examples: Integrated playbook, isolation procedures, drill record, after action items.

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

[LL-HC2] Participate in Cross Entity Information Sharing

Control text: Join an information sharing channel relevant to energy and district heating and ensure alerts reach both IT and operations. Share anonymized lessons learned after relevant incidents when legally possible. Record the actions taken from shared alerts.

Why: District operators face similar technologies and threats and SMEs benefit from shared detection and mitigations. Participation improves speed and reduces duplication.

Evidence examples: Membership evidence, alert distribution list, action records, shared advisory summaries.

Legal anchors: NIS2 Art. 21(2)(g), CER Art. 13(1)(f), CER Art. 12(2).

3.2.2. BUILDING OWNERS AND FACILITY MANAGEMENT

[KP-HC5] Inventory Tenant and Third-Party Integrations

Control text: List all integrations into building automation such as energy optimization services tenant dashboards and maintenance apps. Confirm what data and control rights each integration has. Revoke any integration that can change control values without a clear business need.

Why: Building automation ecosystems grow over time and hidden integration creates silent risk. Reducing unnecessary control rights limits attack paths.

Evidence examples: Integration register, data flow notes, access reviews, revoked tokens or accounts.

Legal anchors: NIS2 Art. 21(2)(i), GDPR Art. 25(1), GDPR Art. 32(1)(b).

[SB-HC6] Remove Default Credentials and Disable Unused BMS Services

Control text: During commissioning verify that every controller and gateway has unique credentials and that unused services are disabled. Document the baseline configuration for each building. Recheck after major maintenance or vendor visits

Why: Default credentials and open services remain common in building incidents. A simple baseline check prevents many avoidable compromises.

Evidence examples: Commissioning checklist, baseline config snapshots, recheck records, vendor acceptance sign off.

Legal anchors: NIS2 Art. 21(2)(i), NIS2 Art. 21(2)(e), RED Art. 3(3)(d).

[SB-HC7] Maintain Privacy and Security Governance for Metering and Occupant Data

Control text: Define who owns metering and occupancy data and how long it is kept and who can access it. Review data access at least yearly and after any new app or integration. Ensure staff understand the rules.

Why: Heating and cooling data can reveal occupancy patterns and business activity. Governance reduces privacy risk and strengthens trust with tenants.

Evidence examples: Data governance notes, retention settings, annual access review, staff briefing record.

Legal anchors: GDPR Art. 25(1), GDPR Art. 32(1)(d), Data Act Art. 4(5).

[WP-HC4] Validate BMS Sensor and Meter Integrity

Control text: Implement periodic checks that key sensors and heat meters are plausible and consistent with expected building behavior. Flag sudden calibration shifts and persistent outliers. Investigate integrity issues before using the data for billing or automated optimization.

Why: Sensor manipulation can drive wrong automation decisions and billing disputes. Simple plausibility controls reduce both cyber and quality risk.

Evidence examples: Validation rules, exception reports, investigation records, corrected data notes.

Legal anchors: NIS2 Art. 21(2)(f), GDPR Art. 32(1)(b), Data Act Art. 11(1).

[RR-HC4] Restore Building Automation from Known Good Baselines

Control text: Maintain a baseline configuration for each building and define a step by step restore method for controllers and gateways. Keep spare devices or images for critical sites where replacement is faster than repair. Validate restore time during a maintenance window.

Why: Building systems are vendor diverse and recovery can be slow without baselines. Faster restore reduces occupant impact and contractor costs.

Evidence examples: Baseline pack per building, spare inventory, restore runbook, restore test record.

Legal anchors: NIS2 Art. 21(2)(c), NIS2 Art. 21(2)(e), GDPR Art. 32(1)(c).

3.2.3. EQUIPMENT MANUFACTURERS AND INSTALLERS

[KP-HC6] Maintain Product Cybersecurity Risk File per Model

Control text: For each connected controller gateway or thermostat model keep a documented cyber risk assessment tied to intended use and typical environments. Update it during the support period when you learn new vulnerabilities or misuse patterns. Use it to decide default settings and update strategy.

Why: Product risks change after deployment and small manufacturers need a lightweight but continuous process. This supports consistent security decisions across variants.

Evidence examples: Risk file per model, update history, design decisions linked to risks, support period definition.

Legal anchors: CRA Art. 13(2), CRA Art. 13(3), CRA Art. 13(7).

[SB-HC8] Secure by Default Update and Recovery Mechanisms

Control text: Provide a secure update method that verifies authenticity and integrity before installation and supports safe rollback. Ensure devices ship with secure defaults that minimize exposed services. Provide installers with a secure commissioning guide that enforces these defaults.

Why: Devices must be updateable without creating new risks and recovery must avoid unsafe states. Secure defaults reduce field misconfiguration.

Evidence examples: Update design description, signing evidence, rollback test record, commissioning guide.

Legal anchors: CRA Art. 13(1), CRA Art. 13(2), RED Art. 3(3)(e).

[WP-HC5] Operate a Vulnerability Intake and Triage Process

Control text: Provide a clear channel for vulnerability reports and define who triages and how fast. Track vulnerabilities per product model and decide remediation or risk acceptance. Communicate fix availability to customers and installers using structured advisories.

Why: Connected devices are widely deployed and vulnerabilities can spread fast across identical models. A formal process protects customers and supports compliance.

Evidence examples: Vulnerability policy, ticketing records, advisories, remediation timelines.

Legal anchors: CRA Art. 13(6), CRA Art. 13(7), CRA Art. 14(1).

[RR-HC5] Notify Customers of Actively Exploited Issues

Control text: When you learn of an actively exploited vulnerability or a severe incident affecting your product, inform impacted users quickly and provide mitigations. Maintain templates that

include what to do now and how to update safely. Track confirmations from key customers when the issue is high risk.

Why: Fast customer notification limits exploitation spread across installed base. Clear instructions reduce unsafe field actions.

Evidence examples: Notification templates, customer mailing logs, mitigation guidance, confirmation records.

Legal anchors: CRA Art. 14(1), CRA Art. 14(2), CRA Art. 14(8).

[LL-HC3] Commit to Support Period Transparency and End of Support Controls

Control text: Publish the support period for each connected product model and define what happens at end of support. Provide guidance for replacement or secure decommissioning. Ensure installers communicate this to customers at sale or installation.

Why: Devices are long lived and unsupported software becomes a sector wide vulnerability. Transparency enables customers to plan and reduces unmanaged legacy.

Evidence examples: Public support policy, product model list with dates, end of support notices, installer scripts.

Legal anchors: CRA Art. 13(3), CRA Art. 13(8), NIS2 Art. 21(2)(e)

3.2.4. ENERGY SERVICE COMPANIES AND AGGREGATORS

[KP-HC7] Identify Optimization and Demand Response Abuse Scenarios

Control text: Document on how attackers could abuse optimization logic such as weather curves pricing signals or demand response commands to cause customer harm or grid stress. Decide which scenarios require detection controls and which require hard limits. Validate the scenarios with operations staff.

Why: Optimization platforms can magnify the effect of a single compromise. Scenario based analysis prevents blind spots.

Evidence examples: Abuse scenario list, control selection notes, validation workshop notes, configured limits.

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

[SB-HC9] Protect Customer Control Rights and Data Sharing Interfaces

Control text: Ensure customer portals and APIs enforce least privilege so users can only access their own sites and only approved control actions. Apply rate limits and strong authentication to prevent automated abuse. Review access roles quarterly for shared accounts and partners.

Why: Platforms often combine customer data with operational control and weak portal controls can lead to disruption and privacy impact. Strong interface controls reduce exposure.

Evidence examples: Role matrix, API authentication settings, quarterly review minutes, access revocation logs.

Legal anchors: GDPR Art. 25(2), GDPR Art. 32(1)(b), Data Act Art. 4(1).

[WP-HC6] Detect Control Command Abuse at Platform Level

Control text: Log all control commands issued by the platform and detect unusual volumes unusual timing or commands that exceed expected limits. Automatically block risky sequences and require human review for high impact actions. Keep evidence of blocks and approvals.

Why: Platform compromise can scale quickly across many customer sites. Command abuse detection reduces systemic risk.

Evidence examples: Command logs, detection rules, block events, approval records.

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

[RR-HC6] Maintain Safe Mode for Optimization and Remote Control

Control text: Implement a safe mode that stops non-essential optimization and limits remote control to essential functions during incidents. Define entry and exit criteria and who can authorize them. Validate that safe mode keeps basic comfort and safety objectives.

Why: During incidents, continuing optimization can amplify harm across many sites. Safe mode limits blast radius while preserving essential operation.

Evidence examples: Safe mode design, criteria document, test results, incident records showing activation.

Legal anchors: NIS2 Art. 21(2)(c), NIS2 Art. 21(2)(b), GDPR Art. 32(1)(b).

[LL-HC4] Measure and Improve Security Outcomes for Optimization Services

Control text: Track metrics such as time to revoke access time to detect abnormal commands and restore time for customer service. Review trends quarterly and decide one improvement action each quarter. Share results with management.

Why: SMEs need simple indicators to keep security work pragmatic. Metrics tie cyber controls to service reliability.

Evidence examples: Metrics dashboard, quarterly review notes, improvement backlog, management updates.

Legal anchors: NIS2 Art. 21(2)(f), NIS2 Art. 21(2)(c), GDPR Art. 32(1)(d).).