MITSUBISHI ELECTRIC · PRACTICAL CYBER × DACTA × APEXAGEN

CCoP & Remote Access

What the Code actually requires of a BMS vendor — and what remote access really costs

Practical Cyber

DACTA

APEXAGEN TECHNOLOGY

Your client asked two things.

"What does CCoP require of us — clause by clause?" · "What remote access is possible, and what does it cost extra?"

What CCoP is

Who issues it

The **Commissioner of Cybersecurity**, under s.11(1)(a) of the Cybersecurity Act 2018.

What it is

Not guidance — the **legally binding minimum** for owners of designated CII.

Version in force

2nd Edition, Revision One (from 4 Jul 2022). 11 sections, ~220 auditable clauses.

Who it binds

The **CII owner ("CIIO")** — water, energy, health, transport, finance, gov…

> **A water-reclamation plant is Water-sector CII — and because it controls a physical process, it's OT CII (Section 10 applies).**

The owner is accountable — and cannot hand that to you.

§3.8.1 — the CIIO "shall remain responsible and accountable… even if it engages an external party." So they discharge it by contract.

1 · The CII operator
Hospital: "vendor remote access shall be MFA & recorded"

▼

2 · The main contractor
passes the clause down, unchanged

▼

3 · You
"connect through our recorded jump host"

One obligation, **three hops** — you deliver to the Act.

So it flows down to you — three clauses

§3.8.1
Accountability **can't be delegated** — they stay on the hook.

§3.8.3
The contract **must stipulate your access**, your obligations, and their **right to audit** you.

§5.1.3
Your access is **constrained by default**: documented, pre-approved, supervised, **on-site**.

> **Fluency here isn't legal trivia — it's how you avoid disqualification at the security gate, and win on trust.**

The clause map — 11 sections

- **§2** Audit · **§3** Governance · **§4** Identification
- **§5** Protection **(the big one — 17 sub-clauses)**
- **§6** Detection · **§7** Response & Recovery
- **§8** Cyber Resiliency · **§9** Training
- **§10** OT Security · **§11** Domain-specific
- Your bid lives in **§3.4/3.5, §4.1, §5, §6.1, §8.1 and all of §10**

1. **Govern**
2. **Identify**
3. **Protect**
4. **Detect**
5. **Respond**
6. **Recover**

CCoP is a **structured lifecycle** — it repeats.

§5 Protection — the cluster that's yours

Access & accounts

5.1–5.3: least privilege, no shared logins, MFA for admin, on-site vendor access.

Network

5.5–5.6: segmented, minimum inter-segment traffic, one-way where possible.

Remote

5.7: disabled unless needed, then the full stack. **See later.**

Hardening

5.9–5.10: no default passwords, patchable, supported firmware.

Applications

5.12: authenticated, secure config, no hard-coded secrets.

Backup

8.1: baseline sequences, alert on change, restorable config.

§10 OT — because a BMS is OT

One-way off the plant (10.2.1)

OT talks to the enterprise net **one-way only** — telemetry out, nothing back in.

Separate credentials (10.2.3)

OT logins ≠ enterprise logins — a stolen office password can't reach the plant.

Fail-safe (10.2.4–5)

On anomaly, the process goes to a **safe state** and alerts.

Secure coding + field controllers (10.3–10.4)

Firmware & programme-code integrity, interlocks, validated inputs, **no rogue writes**, monitored baselines.

> **Your DDC/PLC programming is named in the Code. This is your deepest credential — and your biggest liability if ignored.**

The gold standard — thorough, and expensive.

Every box on that drawing earns its place against a clause — none of it is wasted. The real question isn't "is it too much?" — it's "which parts are ours to price?"

The reference architecture, decoded

Monitoring net (CSM) + data diode

One-way telemetry to the SOC — §6.1/6.2, §5.6.2b, §10.2.1.

DMZ: proxy + remote-access broker

The secured intermediary for any remote access — §5.7, §5.5.

Plant Monitoring net: servers, DCs, historian

Hardening, DBs, accounts — §5.4/5.9/5.13/5.2–5.3.

Automation net + redundant controllers

Control + standby, dual-path (PRP) — §3.5, §10.2.4.

> **Client-neutral throughout — "a water-sector CII reference architecture." Live infrastructure gets handled with discretion.**

Whose scope is it, really?

ME BUILDS & PRICES

- Segmentation-ready, hardened BMS
- Secure controller programming (§10.3/10.4)
- Asset register, config backups, logs
- A jump host **only if** ME supplies it (Tier 2)

OWNER / SI PROVIDES

- DMZ, firewalls, the **data diode**
- The monitoring net & SOC
- The enterprise remote-access broker
- PAM platform licence (Tier 3)

> **The mis-scope trap: saying "yes, we'll do all this" and quietly pricing the whole CII stack into a BMS bid.**

THE HEADLINE QUESTION

Remote Access

What's possible, what the Code demands — and what each option costs extra.

For a CII, on-site is the default. Remote is the exception.

§5.1.3 — all vendor access shall be documented, pre-approved, supervised, and performed on-site. Remote must be specifically permitted and risk-assessed.

When remote is permitted — the §5.7.2 stack

DISABLED DEFAULT	On unless the owner decides it's necessary (5.7.2a).
MFA	Multi-factor to establish the connection (5.7.2b).
SECURED INTERMEDIARY	Strong encryption through a **jump / bastion host** (5.7.2c).
INTEGRITY + SCAN	Transmission integrity; uploads malware-scanned (5.7.2d–e).
MINIMUM FLOW	Only the data the task needs (5.7.2f).
PRIVILEGED	From a **hardened environment**, MFA (5.3.1). Telemetry out one-way (5.6.2b/10.2.1).

The options ladder — priced by cost drivers, not guesses

Tier 0 · On-site only + one-way telemetry

The CCoP default. Lowest cyber risk & kit; ↑↑ **opex** (truck rolls).

Tier 1 · Ride the owner's broker

Request-based via their rig. Low ME cost; best value on a built-out site.

Tier 2 · ME-supplied hardened jump host

MFA + session logging. **Capex + integ** one-time; modest opex.

Tier 3 · PAM + session recording

Vaulting, just-in-time, full recording. ↑ **licence** (usually owner-owned).

> **Tier 4 = the full DMZ + diode + SOC pattern on the drawing — overwhelmingly the owner's / SI's to build. ME integrates; ME doesn't price it.**

Who pays for what — say it out loud

TYPICALLY ME'S COST

- Hardened, segmentation-ready BMS
- Secure controller programming
- Asset register, backups, logs
- Jump host **if ME supplies** (Tier 2)

TYPICALLY OWNER / SI'S COST

- DMZ, firewalls, **data diode**
- Monitoring net + SOC
- Enterprise remote-access broker
- PAM platform licence (Tier 3)

> **Exact numbers need a quote against the specific site. What you carry into the room is the structure, not a guessed figure.**

What to say when they ask

"What remote access can you give us?"

"On-site is the Code's default; where you permit remote, it's request-based — MFA, through a hardened jump host you approve, session-logged, monitoring one-way only. We'll ride your broker, or supply a hardened one."

"Is all this necessary — isn't it a lot?"

"It's the gold standard for a CII — every layer maps to a clause, and it's genuinely expensive. Most of it is your / your SI's scope, not ours. Our part is the BMS to the same bar — and we'll help you spend where it counts."

Tender clauses → your winning answer

"Remote access shall use MFA and be logged."

Per-engineer, MFA, recorded jump host, request-based — never a standing back-door (5.7.2, 6.1).

"Vendor access controlled, time-limited, auditable."

On-site by default (5.1.3); remote is time-boxed, recorded, fully attributable.

"OT segmented from corporate networks."

BMS on its own OT segment; telemetry one-way only (5.5, 10.2.1).

"Field controllers secured against modification."

Integrity-checked code, interlocks, validated inputs, no rogue writes (10.3, 10.4).

Every claim you make, you must be able to defend.

Precision about who is governed and why is what makes you the expert. Overclaim once and a savvy buyer checks — and you lose the room. Decision Survivability applies to sales too.

On-site by default. Remote by exception. Priced by clause.

Grab this deck to keep → bms.ethanseow.com

Practical Cyber

DACTA

APEXAGEN TECHNOLOGY