Preptorum

CONTROL-ROOM HANDOVER AND CALL TREE

EXAMPLE PACK: GRIDTORUM PLC
DOCUMENT 04
FICTIONAL · NOT A REAL COMPANY

GridTorum PLC · Continuity pack document 04

> **FICTIONAL EXAMPLE CONTENT – GridTorum PLC is not a real company.** Roles only, no names. All phone numbers are placeholders. A real company replaces them with its own contact sheet and its own control-room procedures.

1. TWO CONTROL ROOMS, ONE NETWORK

GridTorum runs the network from the **primary control room (PCR)**. The **backup control room (BCR)** is at a separate site, staffed on every shift and able to take control of the whole network. An open incident never pauses: it is handed over, with one owner at every moment.

SITUATION	CONTROL HELD BY	NOTES
Normal running	PCR	BCR watches the same network and keeps its displays and paper diagrams current
PCR systems degraded but room usable	PCR	BCR on the incident bridge, ready to take control
PCR unusable (evacuation, loss of site, loss of its systems)	BCR	Transfer of control under section 3
Shift change during an incident	Whichever room holds control	Shift handover under section 2

2. SHIFT HANDOVER DURING AN INCIDENT

The outgoing Incident Lead reads this checklist out, face to face where possible. The incoming Incident Lead confirms each item.

- ☐ **Status:** incident type, start time, what is affected, current operating mode (Normal, Degraded, Blind).
- ☐ **Network picture:** snapshot time, what is confirmed, reported and assumed, and sites not yet seen.
- ☐ **Faults:** open faults, their priority, and crews assigned.
- ☐ **Fault intake:** which fallback channels are open, and who is posted where with what reporting times.
- ☐ **Switching and permits:** switching in progress, permits issued, isolations in place.
- ☐ **Technology:** cause if known, failover state, current recovery estimate.
- ☐ **Communications:** what government, the regulator, partners and the public have been told, and when the next update is due.
- ☐ **Open actions:** each with an owner and a due time.
- ☐ **Log:** paper log passed over, with the last entry signed by the outgoing lead.
- ☐ **Words of handover:** "You have the incident" / "I have the incident", said out loud and written in the log with the time.

Staff welfare: in long incidents, plan shift lengths, rest and food from the first hour. Tired people make switching errors.

3. TRANSFER OF CONTROL FROM PCR TO BCR

1. **Decide.** The Incident Lead in the PCR, or the Duty Director if the PCR cannot be reached, decides to transfer control.
2. **Warn.** Tell the BCR on the bridge and by direct line. Tell all sites, crews and DNOs that control is moving and when.
3. **Freeze.** Pause all non-urgent switching during the transfer. Make work in progress safe under the safety rules.
4. **Hand over.** Read the section 2 checklist over the direct line or radio. Send photographs of the board and log pages if any channel allows it.
5. **Take control.** The BCR Incident Lead says "BCR has control" on the bridge and writes it in the log with the time. The PCR confirms.
6. **Tell everyone.** Sites, crews, DNOs and generators are told to report to the BCR from now on.

If the PCR is lost without warning, the BCR takes control as soon as it knows, using the last snapshot and its own paper diagrams, and records the time it took control.

4. OUT-OF-BAND CHANNELS

Used when email, Teams, company sign-in or normal phones cannot be trusted.

CHANNEL	USE	WHERE DETAILS ARE KEPT
Direct control-room lines between PCR and BCR	Control and handover	Printed in both control rooms and on the drive
Conference bridge with a provider outside our main platforms	Main incident bridge	Contact sheet on the drive and in the incident folder
Operational radio network	Substations, crews and staff posted at sites	Radio net plan on the drive
Satellite phones	Control rooms, key sites, Duty Director	Incident cabinet in each control room
SMS cascade from company and personal mobiles	First alert and fixed-time updates	Call tree below

5. CALL TREE (ROLES ONLY)

The person who spots the problem calls **Level 1**. Each person calls the people beneath them, then reports back that the calls are done. If someone does not answer within 5 minutes (example), call their stand-in and move on.

LEVEL	ROLE	PCR	BCR
1	Duty Incident Lead (Senior Control Engineer)	+44 1XXX XXXXXX	+44 1XXX XXXXXX
2	Duty Director	+44 7XXX XXXXXX	+44 7XXX XXXXXX
2	Network Picture Lead	+44 1XXX XXXXXX	+44 1XXX XXXXXX
2	Senior Authorised Person on duty	+44 7XXX XXXXXX	+44 7XXX XXXXXX
2	IT On-Call Lead and OT On-Call Lead	+44 1XXX XXXXXX	+44 1XXX XXXXXX
3	Field Operations Duty Manager	+44 7XXX XXXXXX	+44 7XXX XXXXXX
3	Partner Liaison Lead	+44 1XXX XXXXXX	+44 1XXX XXXXXX
3	Cyber response lead	+44 1XXX XXXXXX	+44 1XXX XXXXXX
3	Communications Lead	+44 1XXX XXXXXX	+44 1XXX XXXXXX
3	Government and Regulatory Liaison Officer	+44 1XXX XXXXXX	+44 1XXX XXXXXX
4	Chief Executive delegate	+44 7XXX XXXXXX	+44 7XXX XXXXXX
4	DNO control rooms and generators	Partner contact sheet	Partner contact sheet
4	Cloud and telecoms provider support (AWS, Microsoft)	Account contact sheet	Account contact sheet

First SMS alert (template): "GridTorum INCIDENT: [type] since [time]. Mode: [Normal/Degraded/Blind]. Control: [PCR/BCR]. Join bridge [number], PIN [XXXX]. Do not use email/Teams for this incident. Next update [time]."

6. KEEPING THIS CURRENT

- Each role holder checks their own entries monthly (example).
- The document owner runs a test cascade each quarter (example) and records how long it took to reach Level 3.
- Practise a PCR to BCR transfer on a set schedule and record what slowed it down.
- Update the drive copy the same day a contact changes. The drive holds only what our own staff put on it, so the document owner records the date of every update on the drive.

7. KEEPING THE DRIVES UNDER CONTROL

Procedures only. A real company sets these out in its own policy.

- **Who holds a drive:** the duty Incident Lead and Senior Authorised Person in each control room, the Duty Director, the Field Operations Duty Manager, the IT and OT On-Call Leads, and each staffed key site (example list). Each drive is numbered and signed for in a register.
- **Spare drives:** kept in a locked incident cabinet in the PCR, the BCR and each key site (example), checked against the register each quarter (example).

- **Updates:** the document owner refreshes every drive on a set schedule and after every change to the pack, and records the date and drive number.
- **Returns:** drives are handed back when someone changes role or leaves, and the register is updated the same day.
- **If a drive is lost or stolen:** tell the document owner at once; record the drive number, when and where it was last seen; change any bridge PINs or access codes held in the pack; issue a replacement; and review whether anyone outside the company needs to be told under our own procedures.