Incident response runbook

Operation: Home Front

Transport and logistics · v1.0 · issued 03/05/2026

DOCUMENT CONTROL

Document ID	RB-REMOTE-WORKI-001
Owner	Incident Response Lead
Issued	3 May 2026
Version	1.0 (initial draft from tabletop)
Review cycle	Every 6 months or after any invocation
Classification	Internal — restricted to IR team and leadership
Aligned to	ITIL 4 Incident Management · NIST SP 800-61r2 · ISO/IEC 27035

SCENARIO SUMMARY

This runbook has been created to respond to a home and remote working incident — specifically the "Operation: Home Front" scenario — affecting the organisation in the transport and logistics sector. It was drafted from a tabletop exercise rehearsal and should be treated as a working operational procedure, not a finished plan.

Scenario narrative: Your organisation supports flexible and remote working. An employee working from home has their home broadband router compromised by an attacker who uses it to intercept network traffic. The employee has been accessing corporate systems, email, and sensitive documents over this compromised connection for several days before the issue is detected.

1. PURPOSE AND SCOPE

This runbook directs the response to a home and remote working incident affecting transport and logistics operations. It defines triggers, roles, and the sequenced actions needed to detect, contain, eradicate, recover from and learn from the incident. It does not replace the wider Incident Response Plan, business continuity plan, or legal/regulatory obligations — it complements them.

In scope:

- Assess the security controls your organisation has for remote working
- Evaluate your ability to detect and respond to a compromised remote connection
- Consider the balance between remote working flexibility and security
- Test your response when the breach occurs outside your direct infrastructure

2. ACTIVATION CRITERIA AND TRIGGERS

Invoke this runbook when ANY of the following triggers are observed. The first responder logs the incident in the ITSM tool and pages the on-call Incident Manager.

- Confirmed or suspected home and remote working affecting production systems, staff or customers.
- Detection alert from monitoring (SIEM, EDR, physical alarm, service desk, third-party notification).
- Credible external report from a regulator, partner, supplier, customer or law-enforcement agency.

- Any event meeting the organisation's major-incident criteria (Sev-1 or Sev-2).

3. SEVERITY AND PRIORITY (ITIL)

- Sev-1 / Major — widespread outage, safety risk, regulated-data loss. Convene full IR team within 15 minutes.
- Sev-2 / Significant — material business impact contained to one service or site. Convene core IR team within 30 minutes.
- Sev-3 / Minor — limited impact, no data loss, workaround available. Handle in normal incident queue.

4. ROLES AND RESPONSIBILITIES (RACI)

The following roles were defined for this Transport and logistics home and remote working exercise. Names in brackets were assigned by the facilitator on the day; replace blanks before this runbook goes live.

Incident commander
Leads the response, sets priorities and coordinates the crisis team

Deputy incident commander
Supports the commander and takes over when they are unavailable

Communications lead
Manages internal and external messaging throughout the incident

Legal counsel
Advises on regulatory obligations, liability, and evidential requirements

Communications officer
Drafts statements, monitors media, and coordinates press enquiries

People and welfare lead
Considers staff welfare, duty of care, and people implications

Finance lead
Assesses budget impact, cost approvals, and insurance implications

Scribe / note-taker
Records decisions, actions, and timelines for the post-exercise report

Observer (1)
Watches and listens — contributes observations during the debrief

Observer (2)
Watches and listens — contributes observations during the debrief

Operations controller
Manages service delivery, dispatch, and real-time scheduling

Passenger / cargo safety lead
Ensures safety compliance for passengers or freight handling

Chief information security officer
Sets cyber security strategy and advises the board on risk posture

Security operations analyst
Monitors alerts, investigates indicators of compromise, and triages threats

IT operations manager
Manages infrastructure, servers, and network availability during the incident

Digital forensics lead
Preserves evidence, analyses logs, and determines the attack timeline

Data protection officer
Advises on GDPR obligations, breach notification, and data subject rights

Third-party / vendor liaison
Coordinates with external suppliers, managed service providers, and CERTs

Business continuity manager
Activates continuity plans, manages workarounds, and tracks service recovery

Risk manager
Assesses emerging risks and advises on risk appetite during the response

5. PREREQUISITES AND PRE-POSITIONED ASSETS

- Up-to-date asset inventory (CMDB) and network diagrams accessible offline.
- Out-of-band communications channel (phone tree, secondary chat, bridge line).
- Privileged access via break-glass account; MFA tokens available to on-call staff.
- Verified, immutable backups with documented RTO/RPO and a tested restore procedure.
- Pre-approved holding statements for staff, customers, regulators and media.
- Retainer or on-call contract with external IR/forensics provider.

6. RESPONSE PROCEDURE

The steps below were committed to during the tabletop exercise and grouped against NIST SP 800-61r2 phases. Execute in order; record start/end time and decision-maker for each step in the incident log.

Phase — Detection & Analysis

Step 1 — Categorise & Prioritise

NDM A · Sev-3 / Minor

Trigger: Decision point: Immediate containment

Action: Enforce VPN and reset credentials

Require the employee to use a VPN for all connections. Reset their credentials and session tokens. Continue remote working with enhanced monitoring.

Owner: Risk manager, Chief information security officer, Incident commander

Verify: Confirm action completed, record evidence (timestamp, system, screenshot) in the incident log.

Fallbacks if primary action fails: Suspend remote access and investigate fully; Advise the employee and continue monitoring.

Step 2 — Diagnose

NDM P · Sev-2 / Significant

Trigger: Decision point: Escalation and wider risk

Action: Targeted investigation of the 14 at-risk staff

Investigate the 14 staff with the same router model. Brief the CISO and CTO but hold off on board notification until the scope is confirmed.

Owner: Legal counsel, Data protection officer, Incident commander

Verify: Confirm action completed, record evidence (timestamp, system, screenshot) in the incident log.

Fallbacks if primary action fails: Full estate audit and proactive board briefing; Focus on the confirmed compromise only.

Step 3 — Diagnose

NDM P · Sev-3 / Minor

Trigger: Decision point: Regulatory notification

Action: File on time with minimum detail, delay individual notification

Submit a minimal initial report to the ICO within the deadline. Delay individual notification until the investigation is complete so you can provide accurate details.

Owner: Legal counsel, Data protection officer, Incident commander

Verify: Confirm action completed, record evidence (timestamp, system, screenshot) in the incident log.

Fallbacks if primary action fails: File immediately and notify all affected individuals; Seek a deadline extension before filing.

Phase — Containment, Eradication & Recovery

Step 4 — Investigate & Contain

NDM O · Sev-3 / Minor

Trigger: Decision point: Multi-stakeholder communications

Action: Respond to enquiries as they come in

Respond to each audience as they contact you. Provide factual information on a case-by-case basis. Do not issue a proactive all-staff communication.

Owner: Incident commander, Deputy incident commander, Business continuity manager

Verify: Confirm action completed, record evidence (timestamp, system, screenshot) in the incident log.

Fallbacks if primary action fails: Coordinated proactive communications to all audiences; Restrict information to those directly affected.

Step 5 — Investigate & Contain

NDM O · Sev-3 / Minor

Trigger: Decision point: Investing in remote working security

Action: Phased rollout starting with high-risk roles

Approve a phased VPN rollout starting with roles that handle sensitive data. Provide enhanced guidance for other remote workers. Review after six months.

Owner: Incident commander, Deputy incident commander, Business continuity manager

Verify: Confirm action completed, record evidence (timestamp, system, screenshot) in the incident log.

Fallbacks if primary action fails: Full investment in mandatory VPN and device management; Defer investment and rely on updated guidance.

Step 6 — Resolve & Recover

NDM AR · Sev-3 / Minor

Trigger: Decision point: Long-term remote working strategy

Action: Risk-based remote working tiers

Create tiered remote working categories based on role sensitivity. Higher-risk roles get corporate devices and mandatory VPN. Lower-risk roles get enhanced guidance and monitoring.

Owner: IT operations manager, Security operations analyst, Third-party / vendor liaison

Verify: Confirm action completed, record evidence (timestamp, system, screenshot) in the incident log.

Fallbacks if primary action fails: Zero-trust remote access architecture; Maintain current approach with better awareness.

---

7. COMMUNICATIONS PLAN

- Internal: stand up an incident bridge; cadence updates every 30 min (Sev-1) or 60 min (Sev-2).
- Customers: issue holding statement within 1 hour of declaration; update at agreed milestones.
- Regulator: notify within statutory window (e.g. ICO within 72 hours for personal-data breaches).
- Media: route all press enquiries through Communications Lead; do not speculate on cause.
- Suppliers: notify any third party whose service is implicated, in writing, with timestamps.

8. ESCALATION MATRIX

- T+15 min: no Incident Manager confirmed → escalate to Head of IT / Security.
- T+60 min: containment not achieved → escalate to Executive Sponsor and consider external IR retainer.
- T+4 h: customer-facing service still degraded → invoke Business Continuity Plan.
- Any time: legal/regulatory threshold reached → escalate to Legal & Compliance immediately.

9. RECOVERY VALIDATION AND CLOSURE

- Confirm root cause has been addressed (eradication) before declaring recovery.
- Validate restored services against documented success criteria with the service owner.
- Monitor for recurrence for at least one full business cycle (24–72 h depending on service).

- Close the incident in the ITSM tool with category, sub-category and resolution code.
- Transition any outstanding remediation to Problem Management as a Known Error.

10. POST-INCIDENT REVIEW (NIST §3.4)

- Hold a blameless review within 5 working days, chaired by someone outside the response team.
- Capture: timeline, what worked, what didn't, unanswered questions, owner and due date for each action.
- Update this runbook, the IR plan and detection content with the lessons identified.
- Share an executive summary with leadership and an anonymised version with the wider org.

11. REFERENCES

- ITIL 4 — Incident Management practice guide.
- NIST SP 800-61 Revision 2 — Computer Security Incident Handling Guide.
- ISO/IEC 27035-1:2023 — Information security incident management principles.
- NCSC Cyber Assessment Framework (CAF) — outcome-based cyber security guidance.
- Sector-specific obligations (e.g. UK GDPR, NIS Regulations, FCA SYSC, PRA SS1/21).

12. VERSION HISTORY

v1.0 03/05/2026 — Drafted from tabletop exercise. Owner: Incident Response Lead.