Information Security Incident Response Procedure

1. Purpose

This procedure ensures a consistent, effective, and UK legislation compliant approach to identifying, reporting, managing, and resolving information security incidents that may affect our IT and OT infrastructure, business operations, and sensitive data.

2. Scope

This policy applies to:

- All employees, contractors, and third parties with access to company systems
- All IT and OT systems, including SCADA, tank gauging systems, scheduling, delivery software, and customer databases
- Physical and digital data, communications, and infrastructure across terminals, depots, and headquarters

3. Legal and Regulatory Compliance

Ensure actions comply with:

- UK GDPR & Data Protection Act 2018
- NIS Regulations 2018 (if designated OES)
- Computer Misuse Act 1990
- HSE guidelines (relevant to OT safety)
- Cyber Essentials and NCSC Cyber Assessment Framework

4. Responsibilities & Contact Matrix

Stakeholder	Responsibilities	Contact Method
Lithium Systems (IT Provider)	Lead IT incident response, isolate systems, coordinate technical containment and recovery. Available 24/7, although this is not covered under the standard SLA.	Email: support@lithiumsystems.co.uk Phone: 01259 727847
OT Security Lead	Evaluate and manage OT-related threats	Email: max.fyda@oilfast.co.uk Phone: 07708 870361
DPO	Assess GDPR relevance, liaise with ICO	Email:jonathan.stewart@oilfast.co.uk Phone: 01259 727847
HSE Manager	Ensure incident does not compromise safety	Email: Alan.livingston@oilfast.co.uk Phone: 07955 315633
Senior Leadership	Make decisions on incident severity, resource allocation	

All incidents must be escalated to the Incident Response Team (IRT) immediately via support@lithiumsystems.co.uk

5. Incident Response Phases

5.1 Preparation

- Train staff regularly on cyber and OT incident awareness – Currently provided by Knowbe4 through an e-learning platform.
- Maintain updated contact lists and escalation paths.
- Backups tested monthly; failover tested every 6 months
- Verify monitoring systems (SIEM, SCADA logs, EDR) daily

5.2 Identification

Examples of incidents:

- Ransomware alert from antivirus system
- SCADA system showing unexplained valve opening
- Suspicious login from foreign IP to VPN
- Loss/theft of fuel delivery device with login credentials

Initial Actions (All Staff):

- Disconnect device (if safe)
- Report immediately to IT via phone and email
- Do not delete or alter any logs or files

5.3 Reporting & Escalation

- Complete an **Incident Report Form** within 1 hour of discovery
- Email report to IRT and line manager
- If personal data is involved, DPO must be alerted within 1 hour
- OT incidents must include site manager and HSE in escalation

5.4 Triage & Classification

IRT will:

- Determine affected assets and systems
- Assess data type involved (personal, operational, financial)
- Assign a severity level:
    - **Level 1 (Critical)** – Safety or service delivery at risk
    - **Level 2 (Major)** – Sensitive data or core systems affected
    - **Level 3 (Minor)** – Contained breach or attempted compromise

5.5 Containment

- Lithium Systems disables affected user accounts or VPN access
- OT team may isolate systems from the control network
- Shut down infected endpoints only if safe
- Suspend affected services (e.g., scheduling system, ERP) if risk is high

5.6 Eradication & Recovery

- Lithium Systems removes malware, patches vulnerabilities, changes passwords
- Restore from clean backups after full scan
- For OT, perform safety validation before reconnecting equipment
- Resume operations only after authorisation from Lithium Systems, OT, and HSE leads

5.7 Communication

- Internal: Daily updates via secure email/Teams
- External: Communications Manager coordinates responses
- Regulator notifications:
    - ICO (if personal data breach): within 72 hours
    - HSE (if operational safety impact)
    - NCSC (if designated OES)

5.8 Lessons Learned

- IRT conducts post-incident review within 5 business days
- Update:
    - Policies
    - Procedures
    - Training content
    - Technical controls

6. Documentation

- Use the **Incident Timeline & Key Events Log** during all incidents
- Maintain:
  - Incident report
  - Logs and evidence
  - Communications
  - Regulator correspondence
- Store securely for minimum **6 years**

7. Annual Testing

- Conduct full simulation of Level 1 and Level 2 incidents annually
- Include Lithium Systems, OT, HSE, legal, and senior leadership
- Document outcomes and update this procedure accordingly

8. Glossary of Terms

- **DPO** – Data Protection Officer
- **EDR** – Endpoint Detection and Response
- **ERP** – Enterprise Resource Planning
- **GDPR** – General Data Protection Regulation
- **HSE** – Health and Safety Executive
- **ICO** – Information Commissioner's Office
- **IRT** – Incident Response Team
- **IT** – Information Technology
- **NCSC** – National Cyber Security Centre
- **NIS** – Network and Information Systems
- **OES** – Operators of Essential Services
- **OT** – Operational Technology
- **SCADA** – Supervisory Control and Data Acquisition
- **SIEM** – Security Information and Event Management
- **SLA** – Service Level Agreement
- **VPN** – Virtual Private Network