Request under Freedom of Information Act 2000

Thank you for your request for information which we received on Monday 25th November 2024. I am pleased to confirm the following.

General Information:

Do you have a formal Cyber Incident Response Plan (CIRP) in place?

Yes.

Implementation & Training:
How often is your CIRP reviewed and updated?

Annually.

How often do you conduct tabletop exercises?

Yes.

What types of training are provided to staff on incident response and Cyber Incidents?

- General Cybersecurity Awareness Training
- Incident Response Training
- Tabletop Exercises
- Technical Training for IT and Security Teams

CIRP Components:
What are the primary roles and responsibilities defined in your CIRP?

1. Incident Response Coordinator (IRC)
Role: Lead the incident response process.
Responsibilities:

- Coordinate the response team and oversee incident management activities.
- Ensure alignment with the CIRP and organizational goals.
- Maintain documentation of the incident lifecycle.
- Serve as the primary point of contact for escalations and updates.

2. Incident Response Team (IRT)
Role: Execute the CIRP during an incident.
Responsibilities:

- Detect and analyse incidents.
- Implement containment, eradication, and recovery strategies.
- Conduct post-incident reviews and recommend improvements.
- Maintain communication with other stakeholders and teams.

3. Cybersecurity Operations Team
Role: Provide technical expertise during incident detection and mitigation.
Responsibilities:

- Monitor systems and networks for potential threats.
- Analyse security alerts and identify attack vectors.
- Develop and implement containment and remediation strategies.

4. IT Support Team
Role: Assist in restoring and maintaining IT systems during recovery.
Responsibilities:

- Rebuild and patch affected systems.
- Ensure backups are restored and validated.
- Test and verify system functionality post-recovery.

5. Public Relations/Communication Team
Role: Manage internal and external communication during an incident.
Responsibilities:

- Draft and distribute statements to stakeholders, customers, or the public.
- Ensure consistent messaging to avoid misinformation.
- Manage media inquiries and maintain the organization's reputation.

6. Business Continuity Team
Role: Minimize operational disruptions and support recovery efforts.
Responsibilities:

- Identify and prioritize critical business functions.
- Coordinate with IRT to ensure continuity of operations.
- Implement and test disaster recovery plans.

Could you provide an outline or summary of the key headings and sections included in your CIRP?

1. Introduction
2. Roles and Responsibilities
3. Incident Classification
4. Incident Response Lifecycle
5. Communication Plan
6. Incident Documentation and Reporting
7. Tools and Resources
8. Appendices

Communications:

Does your CIRP include communication mechanisms, such as pre-set templates, for internal and external staff during an incident?

Yes.

If you are unhappy with the information received in response to this request, please address your complaint to the Patient Affairs Office at Milton Keynes Hospital NHS Foundation Trust, Standing Way, Eaglestone, Milton Keynes MK6 5LD If, after exhausting our internal process, you are still unhappy with the information received, you may write to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

If you need any further assistance, please do not hesitate to contact us at the address above.

Yours sincerely

Freedom of Information Co-ordinator
For and on behalf of Milton Keynes Hospital NHS Foundation Trust