East of England Ambulance Service NHS Trust

IM&T Secure Area Access Policy

Document Reference	POL051
Document Status	Approved
Version:	V6.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Chief Information Officer	October 2012	IT Security & Resilience Manager
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
Draft V 5.1	12 September 2022	Approved by Information Governance Group
V6.0	17 October 2022	Approved by Compliance and Risk Group

Document Reference	
Recommended at Date	Information Governance Group 12 September 2022
Approved at Date	Compliance and Risk Group 17 October 2022
Valid Until Date	October 2024
Equality Analysis	Completed May 2022
Linked procedural documents	N/A
Dissemination requirements	All IM&T staff
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups.

This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

Paragraph **Page**

Appendices

1. Introduction

Processing information about patients is a fundamental, routine part of that healthcare. IM&T must operate a robust infrastructure in order to provide the required services to Trust staff, and it is essential that key resources are securely located and have the required level of physical access controls in place.

2. Purpose

This policy defines the access policy for secure areas within the organization that have been identified as containing critical or sensitive equipment.

This policy has been developed as a result of the need to achieve a balance between the legitimate business access needs of authorised staff, and the need to maintain an appropriate level of security; and is designed to ensure that only the specified staff have access to secure areas.

3. Duties

3.1 IM&T Management Team

Are to ensure that robust, fit for purpose, technical solutions are in place to ensure secure, and auditable, access.

Are responsible for the issuing, and revocation of access rights to secure areas under their supervision.

3.2 IM&T Operational Staff

Are responsible for ensuring policy is adhered to as stated in Section 6.

4. Definitions

Secure Area: Any area containing key IT equipment (such as servers, switches, stock items, etc)

Token access: Any form of contactless access such as ID card or dedicated token.

5. Development

5.1 Prioritisation of Work

This policy is required as part of the Trust's wider security requirements, and details the requirements outlined in the Information Security and IM&T Operational Security policies.

5.2 Identification of Stakeholders

Stakeholders are all Information Asset Owners.

5.3 Responsibility for Document's Development

The development of this document is the responsibility of the IM&T Security and Resilience Manager, in conjunction with other senior technical managers.

6. Access to Secure Areas

Unrestricted access to the central computer facilities will be confined to designated staff, whose job function requires access to that particular area/equipment.

A list of persons authorised to hold keys or have token access to the suite and to have knowledge of the code required to unset any alarms is included as Appendix D.

A list of persons authorised to enter the secure area unaccompanied is as per Appendix E.

Restricted access to other staff, where there is a specific job function need for such access, will be granted on a temporary basis only by an authorised key holder. All intended work to be fully explained to all parties. A call will be logged on the Service Desk call logging system detailing who is being granted access and why, and the call will be resolved only when the area is checked by a member of IM&T and all keys/tokens returned.

All authorised staff should be aware of the procedures for entering the secure area, and of the security and environmental systems in place such as fire suppression and alarms. It is the responsibility of the Service Delivery Managers to instruct all individuals of these procedures, and they should be clearly displayed in all areas where relevant.

When unoccupied all secure areas must be kept locked and alarmed (if fitted) at all times.

The alarm codes must not be disclosed to any person other than those authorised for access.

In the event of a member of staff who possesses a key leaving the Trust the relevant line manager should withdraw that item and store in locked storage and inform the Service Desk that this has been actioned. Service Desk will then take the appropriate action for recovery or re-allocation. Likewise, anyone with token access will have that access removed, initiated by logging a call with the Estates department.

7. General Housekeeping

The domestic staff do not provide a service to secure areas for security reasons. Therefore, it is the responsibility of all IT assistants to ensure the following:

- All wastepaper is placed in bins and the bin emptied at least on a weekly basis, with rubbish placed outside the door for collection.

- All empty boxes are to be removed and disposed of appropriately, this is particularly important in order to avoid these becoming a fire hazard.

- The suite is kept dust free and vacuumed regularly, the recommendation being that this should be carried out on a weekly basis.

- No items should be placed on the floor in the secure areas but stored on the racking provided in the workroom/storage area.

- Smoking, eating and drinking is not permitted in any part of the secure areas.

7.1 Conduct

Any conduct within secure areas that is deemed to be unreasonable may result in disciplinary action being taken.

8 Dissemination and Implementation

8.1 Dissemination

This policy will be held in the document library and advertised in line with the Trust policy on dissemination of procedural documents.

It will be circulated within IM&T via the senior management team.

8.2 Implementation

Technical and environmental implementation is currently in place in line with this policy, current legislation and best practice.

9 Process for Monitoring Compliance and Effectiveness

Audits will be conducted periodically to ensure these procedures and protocols are being adhered to, failure to comply with these procedures and/or protocols will be deemed as a failure to comply with the policy and may therefore be treated as a disciplinary matter.

10 Standards

This policy is written to ensure compliance with ISO/IEC 27001, the standard for an Information Security Management System.

11 References

ISO27001 - the standard for Information Security Management, Annexe A.11: Physical & Environmental Security

12 Associated Documents

Information Security Policy

IM&T Operational Security Policy

Appendix A: Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Access to secure areas	All IM&T staff	Service Desk call logs will be reviewed to ensure complianc e	Monitoring will be on-going and a report generated at any point on request.	Call export report from the Service Desk call logging system	Reports will be sent to the requesting manager, in all cases reports should be copied to the IM&T Security & Resilience Manager	The IM&T Management Team will evaluate and issue subsequent recommendations and action plans for any or all identified deficiencies, breaches of policies, or improvements	Changes to policy and/or improvements will be implemented in line with the IM&T change control process, lessons learned will be shared with IM&T operational staff and Estates.

Appendix B: Equality Impact Assessment

<table>
<tr><th colspan="2">EIA Cover Sheet</th></tr>
<tr><td>Name of process/policy</td><td>Secure Area Access Policy</td></tr>
<tr><td>Is the process new or existing? If existing, state policy reference number</td><td>POL051</td></tr>
<tr><td>Person responsible for process/policy</td><td>IT Security & Resilience Manager</td></tr>
<tr><td>Directorate and department/section</td><td>IM&T</td></tr>
<tr><td>Name of assessment lead or EIA assessment team members</td><td>IT Security & Resilience Manager</td></tr>
<tr><td>Has consultation taken place?
Was consultation internal or external? (please state below):</td><td>No</td></tr>
<tr><td>The assessment is being made on:</td><td>
<table>
<tr><td>Guidelines</td><td></td></tr>
<tr><td>Written policy involving staff and patients</td><td>X</td></tr>
<tr><td>Strategy</td><td></td></tr>
<tr><td>Changes in practice</td><td></td></tr>
<tr><td>Department changes</td><td></td></tr>
<tr><td>Project plan</td><td></td></tr>
<tr><td>Action plan</td><td></td></tr>
<tr><td colspan="2">Other (please state)
Training programme.</td></tr>
</table>
</td></tr>
</table>

Equality Analysis

What is the aim of the policy/procedure/practice/event?

This policy has been developed as a result of the need to achieve a balance between the legitimate business access needs of authorised staff, and the need to maintain an appropriate level of security; and is designed to ensure that only the specified staff have access to secure areas.

Who does the policy/procedure/practice/event impact on?

Race	□	**Religion/belief**	□	**Marriage/Civil Partnership**	□
Gender	□	**Disability**	□	**Sexual orientation**	□
Age	□	**Gender re-assignment**	□	**Pregnancy/maternity**	□

Who is responsible for monitoring the policy/procedure/practice/event?

IT Security & Resilience Manager

What information is currently available on the impact of this policy/procedure/practice/event?

None

Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event?

No

Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? **No**

Race	□	**Religion/belief**	□	**Marriage/Civil Partnership**	□
Gender	□	**Disability**	□	**Sexual orientation**	□
Age	□	**Gender re-assignment**	□	**Pregnancy/maternity**	□

Please provide evidence:

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? **No**

Race	□	**Religion/belief**	□	**Marriage/Civil Partnership**	□
Gender	□	**Disability**	□	**Sexual orientation**	□
Age	□	**Gender re-assignment**	□	**Pregnancy/maternity**	□

Please provide evidence:

Action Plan/Plans - SMART

Specific

Measurable

Achievable

Relevant

Time Limited

Evaluation Monitoring Plan/how will this be monitored?

Who **IT Security & Resilience Manager**

How **Reports from IT operational staff**

By **Email \ Service Desk reporting system**

Reported to **Head of Live Services**

Appendix C: Authorised persons:

All IM&T staff employed by the Trust
OOH Supervisors (Bedford main server room, zone 1 only)
Airwave
Beckerleg Cabling
BT
Cleric