Secure Area Access Policy

Document Reference	POL051
Document Status	Approved
Version:	V4.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Head of IM&T	July 2017	IM&T Security & Resilience Manager
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
2.0	December 2015	Approved by Executive Leadership Board
3.1	September 2018	Approved by Information Governance Group
4.0	March 2016	Approved by Management Assurance Group

Document Reference	
Recommended at Date	Information Governance Group 26th September 2018
Approved at Date	Management Assurance Group 20 March 2019
Valid Until Date	September 2020
Equality Analysis	February 2019
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.

3.3 Key \ Access Token Holders

Staff with access rights must take precautions to avoid the loss or compromise of keys, access tokens, etc. and should report any loss to their line manager immediately.

3.4 Consultation and Communications with Stakeholders

Consultation with the relevant stakeholders has taken place as part of the Information Asset Ownership process, whereby Information Asset Owners are informed of the security arrangements stated in this policy.

4. Definitions

N/A

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 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 IT suite 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 the IT suite must be kept locked and alarmed (if fitted) at all times.

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

In the event of a member of staff who possesses an access token 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.

6.1 General Housekeeping

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

- All waste paper 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.

6.2 Conduct

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

7 Equality Impact Assessment

This is attached, Executive Summary is in Appendix C

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 Code of Practice for Information Security Management.
Section 7.1 Secure Areas states:-
"…Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference…"

12 Associated Documents

Information Security Policy
IM&T Operational Security Policy

Appendix A – Document Checklist

	Title of document being reviewed:	Yes/No/ N/A	Comments
1.	**Purpose**		
	Are the reasons for the development of the Document stated?	**Y**	
2.	**Definitions**		
	Have all key terms been clearly defined?	**N/A**	
3.	**Consultation**		
	Have relevant stakeholders and/or users been consulted with?	**Y**	
4.	**Equality Impact Assessment**		
	Has the Trust Equality Impact Assessment Screening Form been completed and attached by the author and approved by the responsible Executive Director?	**Y**	
5.	**Monitoring**		
	Has the Monitoring Table been fully completed and attached?	**Y**	
6.	**References/Associated Documents**		
	Are key references cited?	**Y**	
	Are linked documents identified where appropriate?	**Y**	
6.	**Approval**		
	Does the Document identify which committee/group will approve it?	**Y**	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	**Y**	
	Does the plan include the necessary training/support to ensure compliance?	**Y**	
8.	**Review Date**		
	Is the review date identified?	**Y**	

Information Governance Lead (or delegated authority)			
This Procedural Document complies with the Policy for the Development of Procedural Documents			
Name		Date	
Clinical Quality Team			
The Procedural Documents complies with the relevant NHSLA standards			
Name		Date	

Appendix B – 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 compliance	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 poliocies, 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 C - Equality Impact Assessment: Executive Summary

Executive Summary Page for Equality Impact Assessment:	
Document Reference:	Document Title: **IM&T Secure Area Access Policy**
Assessment Date:	Document Type: **Policy**
Responsible Director: **Director of Strategy and Sustainability**	Lead Manager: **IM&T Security & Resilience Manager**
Conclusion of Equality Impact Assessment:	
Recommendations for Action Plan: **None**	
Risks Identified:	
Approved by a member of the executive team:	
YES	**NO**
Name: **Clare Chambers**	Position: **Head of IM&T**
Signature: **Approved via Email**	Date: **4th February 2019**

This whole document should be stored with the master document and a final approved electronic copy must be sent to the Equality & Diversity Lead at Bedford Office

Appendix D - Authorised persons:

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