South East Coast Ambulance Service NHS
NHS Foundation Trust

Security Audit Procedure

Contents

1 Scope

1.1. This procedure exists to set the protocols of periodic security audit within "The Trust" (South East Coast Ambulance Service NHS Foundation Trust).

1.2. To ensure the process is sufficiently robust and is monitored effectively. The Trust will be able to provide assurance internally and externally of the security arrangements for staff, property, vehicles, medicines, and other assets are regularly monitored and audited by this process.

1.3. This document will define the correct processes to review and conduct a "Security Audit" (Timely security review of all security arrangements on site) These audits are required to be submitted every other month for all location types considered as Ambulance Stations, Make Ready Centres, Emergency Operational Centres, Offices, Fleet Workshops/Centres. Audits are submitted annually are Ambulance Community Response Posts.

2 Site Security

2.1. The security of trust sites is a continual function which requires continuous monitoring to ensure the risks related to the safety and security of staff, property, vehicles, and other assets is managed appropriately. There are eight key areas of consideration Senior Managers responsible for sites should be aware of and promote the culture of responsibility to all staff and forms the basis for the security audits.

2.2. Section 1 Medicines / Medical Gases

2.2.1. The Trust holds a licence to store and administer various medicines and controlled drugs. These must be robustly secured, and spot checked to ensure the medicines / medical gases are only accessible to the appropriate staff to ensure the trust retains its licence and continues to operate.

2.3. Section 2 Vehicle Security

2.3.1. Vehicle security should always remain a prime focus for any site, ensuring the vehicles are parked optimally and secured reduces the risk of thefts and damage. Vehicle keys must be secured onsite within a lockable key box when the vehicle isn't in use.

2.4. Section 3 Staff / Visitor Security

2.4.1. Ongoing effective arrangements to manage staff, contractors and visitors' access will ensure those who are not recognised or authorised are appropriately challenged. A strong security culture should be a fundamental aspect to ensure staff safety on site.

2.5. Section 4 Access to site

2.5.1. Access arrangements are a paramount function for any site to operate effectively and security must be appropriately maintained. Access codes, keys (both site and vehicle) etc. must be kept strictly secure and in full compliance with relevant legislation and governance. A visitor’s log needs to be completed for any staff not swiping in and out of a trust building for security and fire safety.

2.6. Section 5 Grounds/Perimeter Security

2.6.1. Perimeter security should be the first focus for any site, more effective arrangements within this area will require less complex management of other aspects of the site, and will reduce any risks associated with staff, property, and assets.

2.7. Section 6 Building/Station Security

2.7.1. Any site needs to ensure general security around station, doors must be secured, garage shutters closed when not in use. Offices that contain staff/patient records should also be secured when unoccupied.

2.8. Section 7 Information Security

2.8.1. Any site retaining information or records relating to the trust or arrangements related to staff/visitor safety or site risks needs to ensure appropriate arrangements in place. Additionally, to fulfil statutory obligations protected information that may be contained on computers or Patient Clinical Records, must be handled securely. Security Alerts must be stored within the security folder on site.

2.9. Section 8 Property

2.9.1. Property is often a target for theft and is a risk which may impact on staff, the Trust, visitors, and patients. Trust property should be kept tidy and secure in appropriate storage to protect assets, Staff members personal possessions should always be secured in the provided lockers where available.

3 Security Audit Process

3.1. OU Managers who assume responsibility for the site must ensure an audit has been completed every other month/annually for each site under their control. If a deputy is appointed to complete, they must be suitable and capable to carry out the assessment. It is encouraged that the assessing manager includes staff on site in providing input into the assessment to promote a strong security culture.

3.2. The sections referred to in 2.1. – 2.9. above form the security audit which are required to be assessed and commented on the online MS Teams form – Security Audit (Security Audit (office.com))

3.3. All sections must be completed except any section of the security audit doesn’t apply to that site.

3.4. Audits are now completed online using MS Teams form available from the Health, Safety & Security Intranet Site. Any queries arising relating to the audit process will be reviewed by the Security Coordinator and collate any submitted audits within Dashboard/reports on a timely basis.

3.5. Any outcomes and recommendations/actions arising from any submitted security audit will be published back to each site manager indicating any work to be completed within an appropriate timeframe with updates included in the subsequent security audit.

3.6. Local OU Management are responsible for tracking the progress of work and/or actions to be completed. The security coordinator will liaise with local OU Management to offer ongoing support to resolve outstanding works.

3.7. Should any actions arise that are deemed urgent due to any risks identified on a security audit will be escalated to the relevant Operating Unit Manager and Health, Safety & Security Team to mitigate/resolve the risk. These will be formally documented and if appropriate raised to the relevant groups involved.

3.8. Any paper (Appendix A) completed security audits should be retained by the site and stored in the security folder.

4 Responsibilities

4.1. Chief Executive

4.1.1. Ultimately responsible for all policies and procedures within the Trust, including those pertaining to the security of Trust staff, property and assets.

4.2. Security Management Director (SMD)

4.2.1. Responsible for ensuring processes, procedures and systems are in place to manage safety and security on Trust sites to protect Trust staff, property and assets.

4.3. Non-Executive Security Director

4.3.1. Responsible for ensuring that the business of the Trust does not compromise the requirements and directions issued by the Secretary of State, the Department of Health relating to security.

4.4. Head of Health, Safety and Security

4.4.1. Responsible for planning and, following Exec/SMD approval, implementing the strategic direction for site security of Trust sites.

4.5. Security Manager

4.5.1. Responsible for the management of the security audit process, formulating local and strategic recommendations for Trust site security arrangements and where significant risk is identified appropriate escalation and follow up.

4.6. Security Coordinator

4.6.1. Responsible for administration of the security audit process, handling enquiries, coordinating submissions, recommendations, and actions, and supporting the Security Manager with the monitoring of action completion and reviewing the success of the work.

4.7. Managers (Senior / Head Of / Lead / Operating Unit)

4.7.1. Responsible for ensuring a security audit is completed for all sites in their Operating Unit area.

4.7.2. Ensuring they continually familiarise themselves with the principles security to complete or brief a deputy for audit completion.

4.7.3. Strategic level ownership for their Operating Unit's security culture and ensuring suitable Managers are tasked with local actions or following up with other departments, such as Estates.

4.8. Managers (Local / General / Operating / Team Leader)

4.8.1. Responsible for ensuring site security is maintained on a day to day basis and actions from audits are completed or responded to.

4.8.2. Communicating the importance of security on site to all employees, following up on concerns and investigating/escalating security breaches.

4.9. All Employees

4.9.1. Responsible for maintaining safety and security on site for themselves and their colleagues.

4.9.2. Following local procedures to ensure doors, keys, sites etc are left secure.

4.9.3. Ensuring risks to of security are notified to management and breaches reported via a DIF1 Incident Reporting form.

5 Audit and Review

5.1. The Security Manager will continuously monitor the content through its use, to ensure it meets the security requirements of the Trust, whilst remaining relevant and appropriate prior to its scheduled review.

5.2. The procedure will be reviewed every three years or sooner if new legislation, codes of practice or national standards are introduced.

6 References

6.1. Health and Safety at Work Act (1974)
6.2. Misuse of Drugs Regulations (2001)