

PHYSICAL SECURITY POLICY

INTRODUCTION

The EvaStore storage facilities have been designed to securely accommodate client data. The material stored is often highly confidential, politically & commercially sensitive and comprised of medical, legal & financial records & other business critical data. The physical security of the EvaStore warehouses is therefore of paramount importance.

EvaStore warehouses have been designed to offer optimum physical security to protect the assets stored as well as to protect EvaStore facilities against a range of physical threats.

This policy provides a framework which allows EvaStore to operationally manage the physical threats to EvaStore storage facilities.

All personnel working in the office & warehouse will be proactively trained & monitored to adhere & fully comply with this Policy.

SCOPE OF POLICY

The need:

To meet legal and professional requirements as the company must use effective security measures to safeguard physical assets.

To specifically comply with the principle 7 of the Data Protection Act and apply appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

To specifically comply with the Access to Health Records Act 1990 and apply appropriate technical & organisational measures against unauthorised access to health records including deceased patient records.

This Physical Security Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats including theft, criminal damage, fire, flood & pests.

The policy:

The policy of the Company is to accept willingly all obligations in respect of physical security and to protect its resources by implementing recognised best practices.

Effecting this policy requires appropriate levels of physical security such as: - intruder and fire alarms, CCTV, access control, security shutters, security patrols, security lighting and solid building construction.

Applicability:

The policy shall apply to all employees at the Company and any other professional organisation or sole traders using the resources of the company.

PHYSICAL SECURITY POLICY

Implementation:

- The requirements of the policy shall be implemented by all employees and any other professional organisations or sole trader using the company resources.
- Any employees notice any areas of conflict between this Policy and any other policy must bring it to the attention of the General Manager.
- Internal audit shall undertake independent reviews to assess the adequacy of implemented security measures including compliance with the Policy.
- Compliance with the Policy is the duty of all employees.
In serious cases, failure to comply with the Policy must be a disciplinary matter and could also result in a breach of the law or a criminal offence.
- Employees have an obligation to report suspected breaches of the Policy immediately to the Manager Director.

OBJECTIVES OF THE POLICY

The objective of the Policy is to ensure that:

- Resources are protected from accidental or malicious damage.
- Security risks are properly identified, assessed, recorded and managed.
- Processes are in place to reduce risks are implemented at an acceptable cost.
- Prevention, fire and security detection measures for: the perimeters of sites; the Company's buildings or facilities, including all property owned by the Company by rented or otherwise provided, by taking all reasonable measures to prevent unauthorised access.
- Protect against unauthorised access to sensitive materials, both physical and electronic.
- Prohibit unauthorised access to the Company's assets and its information, the Company's customer items and customer information; for the purpose of destroying, disabling, compromising or removing it, with the object of impeding operations, or with the intent of breaching confidentiality, or for financial/personal gain.
- Offer means of prevention, investigation and detection of crime and disciplinary offences in accordance with the Company's disciplinary procedures.

These objectives shall be achieved through the implementation of security controls as described in the remaining sectors of this Policy.

KEY SECURITY CONTROLS

General:

- The Managing Director will ensure that all contracts of employment include a security compliance clause.
- The General Manager and Manager Director will ensure that security responsibilities are allocated to employees and written into their job specification and terms of references.
- Security education and training will be provided to all staff as appropriate to their assessed needs.

PHYSICAL SECURITY POLICY

PHYSICAL SECURITY CONTROL

1. Principle

Resources associated within the company, including office facilities, IT equipment, Warehouse machinery, vehicles and the company buildings shall be protected from unauthorised access, misuse, damage or theft.

2. Access

- Parking facilities are monitored by secure cameras and are designed as secure areas. Visitors are to be escorted at all times within the premises of the buildings and a record of visitors kept in reception.
- In order to prevent unauthorised access during out of hours an Intruder alarm system is provided. Reaction to alarms and subsequent management action are detailed in the company Health and Safety Policy.
- Limits are in place for access to the sites, facilities and building through the use of secured doors & shutters.
- Authorised users shall be supplied with access fobs to gain entry to areas as designed according to their roles and authorisation levels. The Company reserve the right to conduct spot checks to ensure fobs are being carried.
- Request Police assistance in the event of any criminal offence being committed on company's property.

3. Equipment

- All assets held by the company are to be held against an asset register and be uniquely marked as being the property of the company.
- All equipment will be securely stored at the warehouse and will be 'out of bounds' to visitors.
- On-going maintenance arrangements are in place all essential equipment and installation and is subject to review at regular intervals by the IT Manager and Warehouse Manager depending on the equipment.
- Equipment is not to be removed from the building without the authority of the Managing Director.

4. Risk Assessment

- The company is to have a system of Risk Assessment in place to cover all areas of physical security
- Adequate, cost effective controls are to be implemented to reduce the level of associated risk.

INTERNAL SECURITY CONTROL

1. Access Control

- All employees are issued with fobs to access their area of the premises. However, key personnel are issued with fobs which allow them to access all areas of the premises and enable them to access the security shutters, Intruder Alarm and Alarm System with secure Access Code.
- Individuals are to ensure the safe keeping of their fobs to prevent unauthorised access. Any loss of fobs is to be reported to the Manger Director without delay.
- All access to the building and rooms are protected by a security access control. Using the fobs will allow access to users designated area, however allowing others users to enter unauthorised areas is a breach of this policy and will have disciplinary action.

PHYSICAL SECURITY POLICY

2. Security Incident and Reporting

- At the end of each working day, all room occupants are to ensure that windows are fully closed and secured.
- All electrical equipment, with the exception of essential IT equipment (Server, Fax, Telephone system etc.) is to be switched off at the end of each working day.
- At the end of the working day, the warehouse manager is responsible for
 - Ensuring that the Intruder Alarm is set
 - Ensuring fire alarm is active
 - Ensuring that the main door is secured
 - Ensuring that all security shutters are closed
 - Ensuring that all the security doors are shut when leaving the premises

3. Service Continuity Planning

- Physical security is to be incorporated into the company disaster recovery plan to ensure the continued fulfilment of EvaStore services.
- The appropriate intruder alarm systems are implemented, with a link to the alarm response centre & emergency services via BT Redcare GSM/ Digital Communicator. Systems have been designed and installed to a minimum-security grade level 3, by accredited contractors. These systems include vehicle access door alarm contracts & PIR detectors.

FIRE SUPPRESSION

The fire Alarm System conforms to BS 5839:1 2002 and is based upon a category L2 to enhance the safety of occupants by providing warning of smoke within the thoroughfares & escape routes. There is also a gas extinguishant system in the vault storage area utilising HFC227ea (Heptafluoropropane) effective in the protection of electrical hazards. HFC227ea extinguishes a fire by physically weakening & absorbing the heat from a fire. The system has been designed to discharge into the risk in 10 seconds or less.

FLOOD RISK / WATER DAMAGE

The design & location of our storage facilities minimizes the risk of flooding and water damage. All data is stored above ground and above the floor and EvaStore are not located on a flood plain or below the water table. The plumbing systems do not contain pipes that are located in close proximity to data stored and the fire suppression systems do not contain sprinklers. Consequently, the risk of water damage is minimal. Regular inspection and routine maintenance ensures there is no chance of water ingress via the roof or gutters.

PEST CONTROL

EvaStore contracts RSPH Level 2 trained pest control technicians to ensure that prevent infiltration of rodents, insects & other undesirable pests.

EXTERNAL SECURITY CONTROL

1. Security Shutters

- Both buildings EVA1 and EVA2 have been fitted with security shutters on all office/pedestrian doors and office windows. All shutters are to be fully closed when the building is closed.
- All fire exits for both buildings will be kept raised at all times when personnel are in the building.

PHYSICAL SECURITY POLICY

2. Outside Areas

- The exterior of the building and the car park facilities is illuminated by security lights from dusk until dawn. Faults with the external lighting are to be reported to the Managing Director without delay.
- Provision of adequate security lighting in & around the Company's buildings such as loading bays, car park and access routes.
- Suitable out of hour's security guard patrols.
- Comprehensive site-wide CCTV coverage, providing complete internal and external camera coverage of the building and their surroundings.

ROLE OF THE COMPANY GENERAL MANAGER

The Managing Director is responsible for the overall security operation, procuring, arranging or implementing the physical fire and security requirements for the Company.

However, on a day-to-day basis the nominated Security Manager shall be responsible for organising, implementing and managing this policy and its related good working practices.

The nominated General Manager for EvaStore shall:

- Under the direction of the Managing Director, develop and manage the EvaStore security programme
- Develop, issue and maintain the physical security strategy and Policy and agree it.
- Investigate breaches of security and report findings and recommended action to the Company.
- Implement a compliance programme to evaluate the effectiveness of the physical security programme.
- Report annually to the MD on the effectiveness of the overall physical security programme.
- Conduct and record regular security appraisals to ensure acceptable standard of performance these include fire drills, intruder alarm activation test, emergency and security lighting checks, CCTV playback checks.

ROLES FOR EMPLOYEES OF THE COMPANY

Employees of the Company shall be responsible for fire and physical security of their immediate working environment. All employees shall abide by the fire & physical security procedures of the Company. Failure to do so may result in disciplinary action.

Contracts with third party organisation that allow access to the Company's building or facilities shall be in place before access is allowed. These contracts shall ensure that the employees or sub-contractors of those external organisation shall comply with all the appropriate security policies/ guidance required by the Company.

POLICY REVIEW

This policy is to be reviewed on an annual basis by the Security Manager to take account of changing circumstances, legislation, technology and security risks.

Any revisions to the Policy are to be approved by the MD prior to implementation.

PHYSICAL SECURITY POLICY

REPORTING OF INCIDENTS

All data incidents whether large or small need to be investigated to ensure that any lessons that need to be learnt are disseminated to all team members.

The General Manager is to be included in all Data Incidents to ensure that actions that are needed are carried out in the correct timescale.

Reporting of all incidents/issues is to be done via the SE2 Dealing with Issues section within the QMS.

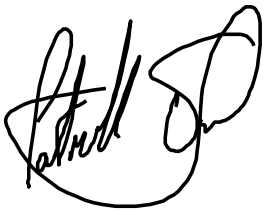
RELATED POLICES

The policy links with, and is to be read in conjunction with, the following:

- Health and Safety Policy
- Information Security Policy
- Quality Policy

Policy approved by:

Signed: 31 January 2023



Patrick Evans

Managing Director