STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	Vaughan House Security
Effective Date:	19 Jun 2019
Reference Number:	SOP-06-06
Version Number:	1.12
Owner:	Information Security Manager,
Review Date:	10 Oct 2021

Table of Contents

1. Purpose

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. Any secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

“Physical security” refers to security measures that are designed to deter or deny access to personnel (including deliberate or accidental intruders), therefore protecting the building, facility, resource, and information from unauthorized use.

This document describes the controls in place for the physical security of the TRE within Vaughan House, including the protocol for requesting access to the building.

2. Scope

The physical security controls for Vaughan House including the process for requesting access to the building are in scope.

3. Responsibilities

The CHI Operational Lead (COL) is responsible for:

- Approving access to Vaughan House
- Storing access requests
- Holding master copy of alarm codes and managing changes to codes
- Responding to alarm code requests
- Holding building master key
- Approving requests to view CCTV footage

4. Procedure

4.1. Introduction

The Trustworthy Research Environment is physically contained within the recently modernised building: Vaughan House. The plans for the refurbished building included the Trustworthy Research Environment and consequently it is physically secure by design.

In accordance with our ISMS policy, the physical security of Vaughan House is periodically reviewed as indicated in the audit calendar and also as a result of unauthorised access incidents.

4.2. Implemented Security Controls

4.2.1. Control on the exterior of the building

Vaughan House is enclosed by buildings and fences on all sides. At the front of Vaughan House, two of the entrance doors are protected by 1.5m high fencing or walls with lockable gates. The main entrance door is through the black gate and up the access ramp and has 24h access by authorized UoM identity (ID) card access, or via the intercom system during office hours. The black gate is locked outside of office hours (0800-1800).

4.2.2. Entrance/exit Doors

There are three ground floor entrance/exit doors:

- The main entrance is the accessible entrance which is accessed through a gate which should be locked outside of office hours (0800-1800) when the building is empty. The main entrance door has an ID card access control system allowing access into the reception area and the alarm control panel.
- The street entrance to the building is a locked black door which is no longer in use and is permanently locked. This door also has an intercom to alert staff to visitors requiring access to the building. Visitors are then asked to go round to the access ramp to gain access to reception.
- The fire exit is through two doors near the toilets on the ground floor which cannot be opened from the outside. These lead to a locked black door which leads to the rear car park, and must be manually opened from the inside.

The gate leading to the main entrance has a lock controlled by a digital key-pad. It is important that this gate is locked outside of office hours when the building is empty, which means the last person leaving the building after 18:00 should ensure the gate is closed [locked] behind them.

On the first floor there is a door from the kitchen to the outside terrace. This is locked with a key and can only be opened from the inside. This door is to remain locked when not in use to prevent unauthorised access from the roof terrace. The key is stored in the cupboard above the fridge.

4.2.3. External Windows

The building has double glazed windows throughout except the Conclave ground floor room and the first floor kitchen. All windows that open have key locks. Please see later sections of this document for guidance on key holders.

4.2.4. Internal Doors – Access Controls

Ground Floor:

- The Congregation Room (G.009) has ID card access control
- The office areas are accessed through an internal entrance door with ID card access control.
- Internal corridor doors close automatically when the fire alarm is triggered
- The Server Room (G.005) has a mechanical key-lock and additional ID card access control
- The office in room G.002 has additional ID card access control
- The Switch Room (G.004) is locked with a key held by UoM estates.
- The Communications Room (G.014) is locked with a key held by UoM IT Services.

First Floor

- Lockable individual occupancy offices (1.004. 1.003 and 1.002)

Second Floor

- The Secure Data Room (2.007) has a mechanical key lock and additional ID card access control (the process for requesting access to this room is described below).
- Lockable individual occupancy offices (2.001, 2.002, 2.003)
- The Plant Room (2.012) is locked with a key held by UoM estates.

4.2.5. Fire exits and Fire Protection

The fire exit route is through two doors that cannot be opened from the outside: the first door, accessed from the ground floor corridor, is opened via the use of a push bar; the second door is opened via the use of a thumb turn lock on the internal side of the doorway.

Each room is fitted with a smoke detector. The fire alarm is tested every Friday at 11:40.

There is a fire safe in the applications development office for the protection of critical items such as backup discs.

4.3. Requesting access

Vaughan House uses a combination of physical keys and authorized UoM ID cards to grant access to the building. All access requests must be recorded in document FORM-005 and stored by the COL. If the requester has a Q-Pulse record the completed form must be attached to the Person record for that individual.

4.3.1. ID Card activation

Vaughan House uses the UoM ID card for access control. By default a UoM ID card will not enable access to the building. Anyone requiring access to Vaughan House will need to request approval from the COL by following the procedure as described here, and on FORM-005:

- The requestor must complete the Vaughan House Access Request form (FORM-005).
- Submit the completed form to the email address defined within FORM-005.
- The COL will assess each access request (consulting the ISSG if necessary) and will approve applications by arranging ID card access with UoM estates.
- UoM estates will make a copy of the latest version of the Vaughan House Access List available to the Information Security Manager on request (e.g. for Routine Measurement and Monitoring).

4.3.2. Access to Secure Areas (Secure Data Room, Server Room)

The secure data areas of Vaughan House are subject to an extra security measures. Access to the data room and server room require a mechanical door lock key and additional ID card approval. The process to request access is as described for standard ID card access to Vaughan House, and again requires completion and submission of FORM-005.

4.3.2.1. Access to TRE Server Room

ID card access and allocation of mechanical door keys KEY-01, KEY-02 and KEY-03 is restricted to the Director of CHI, ISM and TRE System Administrator.

4.3.2.2. Access to the Secure Data Access Room

ID card access is restricted to authorised staff only. The mechanical door keys are stored in TRE-SAFE-02 and the digital code for TRE-SAFE-02 is only known to the same group of authorised staff. When access to this room is required by other individuals, they can only be accompanied by either the ISM or a member of TRE Operations.

4.3.3. Key access

The COL holds the building master key. The occupant of each office has a key for that office, and, where applicable, the windows and personal office storage. Please seek approval for access into locked areas by contacting the individual office occupant or the COL if the occupant is unavailable. Access will only be granted by the COL in emergency situations and will be recorded on Q-Pulse.

4.4. Granting Access to Suppliers

No Vaughan House temporary or spare swipe-cards may be provided to any contractor or supplier. Under normal circumstances where such approval is not granted, the member of staff at CHI who has responsibility for the supplier must make arrangements to open doors and accompany the supplier into any secure locations they need to access.

4.4.1. Supplier Access to the TRE Server Room

Non-TRE staff such as supplier personnel may only enter the TRE server room with prior approval from the TRE Operations Manager or the Health Informatics Programme Manager (TRE). This is to ensure there is full control over any person entering or leaving the TRE server room, and to make sure TRE Staff are available to supervise the supplier.

FORM-009 must be completed by the supplier visiting the TRE Server Room before they gain access.

For non-urgent maintenance arranged by TRE Staff, agreement for the work to commence will be agreed at weekly TRE Development meetings, or via the internal tre-operations@manchester.ac.uk mailbox.

TRE staff and the Director of the Centre for Health Informatics are the only people permitted to be alone in the TRE Server Room. All suppliers must be accompanied by a member of TRE staff at all times.

It is strictly forbidden to lend a TRE Server Room physical key to any supplier.

4.5. Security Systems

4.5.1. CCTV

The building has CCTV cameras covering all four exterior doors and one for each aspect. Internally, the reception area has CCTV coverage. The whole building is protected by a key fob/code entry alarm system with PIR systems in every room.

The CCTV footage is recorded directly onto a DVR located in the Vaughan House reception office. It is only possible to view the content of this DVR using dedicated software. Only UoM Estates Security can install this software, and it is currently only installed on PCs within the Vaughan House reception office.

CCTV footage is retained for 30 days during which time any member of staff can request to view the footage via submission of FORM-005. The COL will review each application and approve or reject requests to view CCTV footage, depending on whether the requestor has a valid reason to do so. CCTV footage will be not released without the COL's approval.

4.5.2. Building Alarm

The building is protected by an alarm system using door release sensors and motion sensors. Outside of office hours when the building is empty the alarm should be set and a code is required to deactivate.

Requesting an alarm code and the main entrance gate code is managed via FORM-005 which will be attached to the person record in Q-Pulse.

The COL holds the master copy of the alarm codes and can generate codes for 3 different role types within Vaughan House:

- Role 1: Permanent members of staff
- Role 2: PhD Students
- Role 3: Research Staff

Once the COL has processed the request, they will arrange to meet the requestor in Vaughan House reception to demonstrate how the alarm system works.
The COL will change the alarm codes periodically. Individual alarm codes are not recorded on Q-Pulse. Allocation of alarm codes is recorded on a secure, password protected spreadsheet.

5. Cross-referenced ISMS Documents

Number	Type	Title
FORM-009	ISMS\Forms	TRE Visitors Access Form
FORM-005	ISMS\Forms	Request for Access to Vaughan House Secure Zones and Security Resources

6. Appendices

None