THE UNIVERSITY of EDINBURGH
Estates Department



Estates Design Guidelines No. 8

Security Services

Important Comment on Estates Design Guidelines, Assets & Standards

These Design Guidelines, Assets and Standards and the associated suite of documents have been produced in order to furnish external design consultants and contractors with guidance on required University standards for inclusion within their proposed project design.

These guidelines are to be used as supplementary information during project design stage, and as such, detail the minimum standards expected from the University Estates Department.

Please note, these guidelines do not absolve the project design team including, sub-consultants and sub-contractors of their legal and contractual obligations under, design liability, statutory regulations and health and safety legislation.

EDG No. 8 Security Services - Approval Procedure	
Estates Design Guidelines No. 8 Security Services Check and Approval – Security Operations Manager	Name: Gareth Satherley Date: 06.04.26
Estates Design Guidelines No. 8 Security Services Check and Approval - Head of Building Services	Name: Sheila Scott Date: 08.04.26
Estates Design Guidelines No. 8 Security Services Approval (Major Policy Changes Only) - Director of Estates Operations	Name: N/A Date:
Estates Design Guidelines No. 8 Security Services Approval (Major Policy Changes Only) - Estates Leadership Team	Name: N/A Date

Version Control for Estates Design Guidelines No. 8 - Security Services

Version	Date	Nature of Revision	Author	Approved by
1.0	June 2026	New Guidelines	KR	SS/GS

Contents

Section

1.0 Introduction 6

1.1 Important Notice – Essential Prior Reading 6

1.2 Purpose of the University of Edinburgh Estates Design Guidelines (Assets and Standards) 6

1.3 Interpretation of UoE Estates Design Guidelines, Assets and Standards 7

1.4 Glossary of Terms: 7

1.5 Review Design Data Process (RDD) 8

1.6 The Obligations Owed 9

1.7 Version Control and Updates 9

1.8 Purpose of UoE Design Guideline Number 8 9

1.9 Legislation and Best Practice Standards for Reference 11

1.10 University Approval Procedures 12

2.0 Security Services – Design Criteria 14

2.1 Design Criteria 14

2.2 Design Criteria 16

2.3 Information Security 17

3.0 Closed Circuit Television (CCTV) System 19

3.1 General Requirements 19

3.2 CCTV Camera Equipment 22

3.3 CCTV System – UoE Network Connection 23

3.4 Stand-alone CCTV Systems 23

3.5 CCTV System – UoE T59 Procedure 24

3.6 CCTV System – Signage 25

3.7 CCTV System – Existing Building Systems 25

4.0 Intruder Alarm Detection System (IADS) 27

4.1 General Requirements 27

4.2 Intruder Alarm Detection System Equipment 27

4.3 Panic / Hold Up Alarm 29

4.4 Intruder Alarm Detection System – UoE T59 Procedure 29

5.0 Final Fire Exit Door Monitoring Systems 32

5.1 General Requirements 32

6.0 Vehicle Barrier and Parking Systems 34

6.1 General Requirements 34

6.2 Barrier Equipment 34

7.0 Appendices 37

7.1 Appendix No.1: Schedule of Existing Assets 37

1.0 Introduction

1.0 Introduction

The UoE Design Guidelines (as a whole), have been developed for employees of the UoE, Design Teams, Architects, Engineers, Project Managers, external consultants and contractors. This documentation has been developed to enable Design Teams and Contractors to have a broad understanding of the principles that the University of Edinburgh will require to be adopted for any future developments.

The guide is primarily designed to be used in conjunction with Royal Institute of British Architects (RIBA) stages. The actual extent and scope of the design guide to be incorporated for any future development will be based upon the specific project requirements.

The UoE Design Guidelines aim to discuss strategic matters and does not provide an exhaustive treatment of statutory or best practice design and compliance requirements; its primary purpose is to establish a starting point for design briefs, support the consultation process and outline existing assets and standards. It is the responsibility of Design Team readers/duty holders to ensure subsequent designs are complete, compliant and able to meet the final approved brief when measured in use.

Reference should be made to the relevant UoE Design Guidelines throughout the Design drawings and documents and Designers should confirm that the appointed Contractors are made aware of the Guidelines to ensure that installations conform to these requirements.

1.1 Important Notice – Essential Prior Reading

It is essential for readers of this document to first refer to Design Guideline No.1 entitled ***"Estates Design Guidelines (Assets & Standards) Introduction and Application"***, which serves to provide the principles and overview with vital information and context that will apply to all projects.

1.2 Purpose of the University of Edinburgh Estates Design Guidelines (Assets and Standards)

The purpose of the Estates Guidelines is to act as a briefing document to give designers an overview of the minimum design requirements, constraints and challenges presented by the University of Edinburgh's particular needs. It applies to all new-build, refurbishment, minor works and change of use projects, including property leased by the University, controlling quality in the production of designs, specifications and the subsequent performance of buildings, developed to a consistently high standard and ensuring continuity throughout the University Estate.

The University of Edinburgh encourages innovation; however, all project Design Teams should ensure that their proposed projects have end user considerations and ease of maintenance at its core.

The use of the University of Edinburgh Estates Guidelines, Assets and Standards will not take the place of, or remove, any of the professional responsibility from Design Teams and Contractors to fully comply with the requirements within this document. Given the complex, diverse and growing estate, not all eventualities can be fully defined within this document.

Should any projects deviate from these guidelines, a technical submittal outlining the deviation, reason why and impact to the University maintenance strategy should be prepared and forwarded to the nominated University project representative for liaison with the UoE Security and Building Services Group (BSG).

A review of this deviation shall be carried out by UoE Security and the BSG; a final decision on the deviation shall be communicated to the appropriate design/construction team.

1.3 Interpretation of UoE Estates Design Guidelines, Assets and Standards

The Estates Design Guidelines, Assets and Standards are required to be issued with all project contractual documentation in order to inform project design and construction teams of expected standards to ensure quality continuity across its Estate.

1.4 Glossary of Terms:

Enforced Requirements

The use of the word(s) ‘shall’, ‘are required’, ‘is required’ ‘must’ or ‘will’ denotes a requirement that is non- negotiable and shall be used as the basis for designs, technical submissions and/or activities. If such a statement conflicts with a statutory obligation then a technical submittal shall be issued to the University project representative for liaison with UoE BSG / Security for their final decision regarding compliance with the documentation.

Requirements Needing Confirmation

The use of the word ‘may’ denotes a negotiable requirement or indication of a solution, where innovation and further calculation, design and discussion may be required to arrive at an optimised solution.

Quality

The Design Guide aims to arrive at the University of Edinburgh's highest design aspirations and standards. It may be that, at the University of Edinburgh's sole discretion, solutions are value managed and then value engineered during subsequent design iterations. Design Teams and Contractors are encouraged to consider where value management and subsequent value engineering may result in an improved financial performance should funding constraints occur. All mechanical and electrical value management and value engineering exercises carried out shall be forwarded to the BSG for review.

Currency of Third Party Documents

Where superseded standards and regulatory documents are referred to in the text, the reader shall apply current revisions and amendments to their project. Should there be any ambiguity, the BSG should be contacted for clarity.

Proof

Where the word 'proof' is used, e.g. 'proof is required', a written report or installation certificate must be produced for approval depending on context.

Assets and standards

The Design Guidelines endeavours to set out Assets and Standards that will maximise the benefits realisation for the UoE to achieve its strategic objectives and maximise value for money. This will involve coordinated and optimised planning in conjunction with Procurement, robust asset selection with particular reference to existing legacy assets and standards on the University Estate, for reasons of utilisation and continuity of maintenance, replacement of parts, renewal and ultimate disposal.

1.5 Review Design Data Process (RDD)

All proposed designs shall be submitted to the Project Manager, respective Estates Teams and Building Services Group for review and comments, the response will be categorised as follows:

A. Design Team to acknowledge comments and continue to develop the design to the next stage.
B. Design Team to acknowledge comments and update the design in accordance with comments and resubmit for consideration before proceeding to the next stage.

C. Design Team to acknowledge comments and completely review and update the design in accordance to the agreed design principles and resubmit for consideration before proceeding to the next stage.

In addition to the above, the UoE may request specific technical submission to support the RDD and may include the request setting out with proof, e.g. calculations, drawings, etc.

The purpose of the RDD is to ensure designs meet the strategic requirements of the UoE and do not compromise the future operations and maintenance provision. The obligations owed by external architects, consultants and contractors to UoE and their liabilities to UoE is not in any way diminished or otherwise reduced by the RDD.

1.6 The Obligations Owed

By external Design Teams, consultants and contractors to University of Edinburgh and their liabilities to University of Edinburgh is not in any way diminished or otherwise reduced by the approval process. University of Edinburgh is not taking over the roles and duties of the external Design Teams, consultants and contractors who will remain legally responsible for the design and/or works carried out by them or on behalf of their staff, agents, sub- consultants and/or sub-contractors.

1.7 Version Control and Updates

The Estates Design Guidelines are to be reviewed and updated by the Electrical Engineering Services Working Group in each calendar year.

The UoE Estates respective Project Management (PM) teams will send e-mail notifications to the Directory of current Design Teams and Contractors appointed, following any update or change.

Any updates to the Design Guidelines, which cause significant change to a project design, should be raised and discussed with the respective Project Management Team and application of the Change Control Process will be required.

Any new items or amended content shall be highlighted in yellow to enable identification of changes from previous versions.

1.8 Purpose of UoE Design Guideline Number 8

The purpose of this document is to set out the guidelines and standards that apply to University of Edinburgh (hereby referred to as UoE) Estate and its design requirement for Security Systems as set out by the Development Services Engineer (Electrical) This document will apply to newly constructed buildings and existing

buildings scheduled to be refurbished. In some cases, this standard exceeds the Building Regulation requirements, as it represents good practice in the Higher Education sector.

The Building (Scotland) Regulations set out to ensure that new buildings and works achieve the objectives of the Building (Scotland) Act 2003 in terms of health, safety, welfare, convenience conservation of fuel, power and sustainable development and the purpose of this guide will be to provide a standard policy specifying the standard that is required by the UoE.

This guidelines document is for designers, engineers, specifiers, installers and commissioning and maintenance engineers of Electrical Engineering Services from Stage (RIBA Stage 2) to when the building is in use (RIBA Stage 7). The design team will be required to align the requirements of the Scottish Buildings Standards Technical Handbook / Building (Scotland) Regulations, fire safety legislation, CDM Regulations, CIBSE Guides and the University

The guidelines document provides an indication of non-prescriptive preferred solutions and appropriate standards. This is not a statement of requirements or intended to replace existing British or European technical standards or national guidance; reference to these will still be necessary.

If due to the nature of the project, certain aspects of Security Systems are not covered in these guidelines and standards, the relevant codes of practices, British Standards and building regulations are to be applied and followed. For any general and specific queries, advice is to be obtained from the Building Services Engineer (Electrical.) In the event those documents referred to within this document, which have been superseded, then most recent versions are to be referred to.

Any other doubts, concerns or points of clarification on Security Systems, please contact the Development Services Engineer (Electrical.)

This document applies to all buildings managed or owned by the UoE. Any tenanted buildings must not have building works, adaptions or change any building or part of a building which will affect the Security Systems or any other building without first receiving permission from Development Services Engineer (Electrical) and the Landlord of the property or nominated agent and written in the respective lease.
This document indicates the University's generic Security Systems Client requirements. Consultants must also refer to specific project requirements identified by the University's Project Manager and they must fully integrate any new Security Systems with the University's existing legacy systems. Consultants and contractors must obtain approval in writing for any variation from these requirements.

Before incorporating these client requirements in, e.g. tender documentation, etc, please always check with the undersigned that you have current issue of both these client requirements and the field equipment list.

Please always approach the University engineers directly to discuss any point of clarification or possible improvement and to obtain further copies of the client requirements.

Development Services Engineer (Electrical)
Estates Operations
Estates Department
Edinburgh
EH1 1NP
General enquires: 0131 650 9157

1.9 Legislation and Best Practice Standards for Reference

Any design must, as a matter of statute, be compliant with the Health and Safety at Work Act 1974, any relevant legislation and associated Approved Codes of Practice (ACOP's.)
Examples of secondary legislation include; the Provision and Use of Work Equipment Regulations 1998 (PUWER), the Workplace (Health, Safety and Welfare) Regulations 1992, the Electrical Safety at Work Regulations 1989, the Control of Major Accident Hazards Regulations 1999, the Confined Spaces Regulations 1997 and the Gas Safety (Installation and Use) Regulations 1998.

Your attention is drawn in particular to the legal duties placed on designers by the Construction (Design and Management) Regulations 2015.

Suitable and sufficient safe access for maintenance and repair must always be provided.
The University will comply with all relevant legislation and regulations relating to the design and structure of the building. Academic, administrative buildings and all residential property are subject to the requirements of the current Technical Standards (Scotland) Regulations/Building Regulations and CIBSE Guides:

Guide A	Environmental Design
Guide B1	Heating
Guide B2	Ventilation and ductwork
Guide B3	Air conditioning and refrigeration
Guide B4	Noise and vibration control for building services systems
Guide C	Reference Data
Guide D	Transportation systems in buildings
Guide E	Fire Safety engineering
Guide F	Energy Efficiency

Guide G	Public health engineering
Guide H	Building control systems
Guide K	Electricity in Buildings
Guide L	Sustainability
Guide M	Maintenance Engineering and Management

These standards allow detailed professional knowledge and judgement to be applied in order to develop a final design solution, which will satisfy projects that are more complicated.

The list of legislations, regulations and guides above is not exhaustive. The Design Team shall prepare and submit project related list as part of RIBA Stage 3 design submission.

1.10 University Approval Procedures

The University governance procedures are described in the Project Delivery Process Map. This includes development of a consultation strategy at RIBA Work Stage 0 and ensuring that there are MEP Design focused consultations with the Estates BSG representatives as part of the project stage approval. Refer to the project T18 document for the schedule of required consultations.

2.0 Security Services – Design Criteria

2.0 Security Services – Design Criteria

2.1 General Requirements

All designs, must, as a matter of statute, be in compliance with all Building Control Regulations, British Standards, CDM Regulations, Health and Safety at Work Act 1974, Electricity at Work Regulations 1989, National Security Inspectorate (NSI) / British Security Industry Association (BSIA) guidance and all associated Approved Codes of Practice.

- The electrical installation associated with security system installation shall be designed and installed in accordance with BS7671 18th Edition IET Wiring Regulations and most current amendment.
- A Departure from the requirements of BS7671 18th Edition IET Wiring Regulations shall be declared by the project Electrical Consultant/Contractor to the BSG and recorded on BS7671 electrical certification for compliance. Departures as rule of thumb will not be accepted by UoE, in particular, Departures caused as a result of design/installation errors. Accepted departures shall include declaration from Designer that the resultant degree of safety is not less than that achieved by full compliance and recorded on electrical installation certification.
- All projects shall be designed and constructed in compliance with the Construction, Design and Management regulations 2015. All project team members should be aware of the legal duties placed upon them during all stages of design and construction, ensuring that all building elements are safe to use and maintain by university personnel.

2.1 Design Criteria

The associated building security services shall be designed in accordance with the following criteria:

- Secure By Design (Consultation with UoE Security team).
- Building Control Regulations and associated Technical Booklets.
- British Standards.
- Estates Design Guide No.11-Sustainable Design instead.
- All University Design Guidelines, with specific attention to future maintenance strategies.
- The requirements of UoE Security Team.
- NSI / BSIA Guidance.
- Flexibility in use and future proofing as far as reasonably practicable.
- System reliability, resilience, maintainability and cost in use.
- Safety of all end users and General Data Protection Regulations (GDPR).

The security of buildings can be considerably enhanced by well thought out design. 'Secured by Design 'is the official police security initiative that works to improve the security of buildings and their immediate surroundings. It is essential that this is considered from the earliest stages. The design team should refer to the appropriate SBD Development & Technical Guides in their design approach. The University Security team can give 'secured by design advice', or can facilitate contact with Police experts.

The Design team shall also liaise with Police Scotland representatives to adopt the principle of "Design Out Crime" during the early design stages.

Design Team and Contractors must exercise due care and competence, in ensuring that all operational compliance requirements are delivered and demonstrated under the University T59 handover procedure.

The following information is intended to provide guidance to those responsible for the design of security system installations within the Estate of the University of Edinburgh.

These Design Guidelines are not intended to be exhaustive or definitive and it will be necessary for users of the guidance to exercise their own professional judgement and competence, when deciding whether to abide by or deviate from it. Any deviations are to be formally captured and issued to the UoE Security / BSG for consideration and approval.

Project design and construction teams shall ensure that all projects are designed and constructed with energy efficiency and future maintenance in mind. Whether it be a new build or refurbishment project, designers should adopt an approach, which recognises the need to:

- Reduce the demand for energy and materials.
- Streamline system requirements and management intervention.
- Encourage the use of, where practicable, renewable energy sources.

Refer to Estates Design Guide No.11-Sustainable Design for further guidance.

The design for the security Services shall generally be deemed to include but shall not be limited to:

- Electrical supplies to security system installations including POE / POE+ systems.
- Containment and wiring systems for security systems.
- External and car park lighting installations designed and coordinated to supplement CCTV clarity and overall coverage.

- Specification of open protocol and compatible security services equipment to match that of existing systems at various UoE Campus locations.
- Door access control systems (in compliance with UoE ISG Guidelines).
- Intruder detection and alarm system.
- Closed Circuit Television (CCTV) Installations (internal / external where applicable).
- Panic / Distress alarm systems.
- Review of existing security services and providing upgrades where required.
- Data and structured cabling installation associated with security systems.
- Testing, commissioning and bringing into service.
- Familiarisation with existing site pre-construction, i.e. site surveys, existing system inspections, etc.
- Building handover – T59 Procedure, Operation and Maintenance (O&M) Manual including all operating instructions and procedures.

Due to the security systems being a critical building safety system, it is the UoE preference where possible that the supply, installation and commissioning of the complete security systems within new buildings is carried out by the UoE incumbent maintenance contractor in order to ensure familiarity with university procedures, this shall be discussed with the UoE BSG prior to tender.

For refurbishments, alterations, or modifications to existing buildings/systems all work associated with the security systems **must** be carried out by the UoE incumbent maintenance contractor to avoid any issues with responsibilities between contractors.

2.2 Design Criteria

Requirements for access control systems should be referenced in Information Services – IT Infrastructure document V2.2 – July 2019. Please note, final consultation with the UoE CIS team is required under the T18 process during design stage to ensure the responsibilities and requirements are understood and incorporated within the contract.

It is the responsibility of the Design Team during design consultations to liaise with the UoE PM and End-Users to determine the operational principles of each internal and external access-controlled door to ensure the correct system and associated door furniture/ironmongery/electrical attendances are included within the design tender documentation.

The use of electronic locking devices across the UoE Estate for both internal/external access-controlled doors shall be discussed at early design stage with the UoE FSU/BSG/ISG and externally via local Building Control, however, as a rule of thumb, maglock devices should be avoided. Final exit doors shall allow free egress at all

times, including during fire alarm/mains failure events, whilst maintaining secure control of ingress to the building.

All access-controlled doors located on internal escape routes shall fail-safe and shall also be provided with appropriate locking hardware to ensure that the locking device is mechanically overridden at all times, refer to UoE Estates Design Guide No.9 for further guidance.

The Design Team shall follow the requirements set out in section 2.9.18 – 21 of the Non-Domestic Technical Standards in relation to the provision of locking mechanism's (including the appropriate overrides) and their application throughout a building.

Access controlled door strategy to be reviewed at an early design stage with nominated End-User groups, UoE BSG/ISG and Security.

2.3 Information Security

Where any system or item of equipment requires access to the UoE IT network either locally or externally, the system software will require to be assessed by UoE Estates IT team to ensure the UoE information security requirements are met. Generally, the requirements of ISO certification ISO27001 for information security management systems shall be followed.

The electrical consultant and contractor are responsible for providing the required security information as required for approval prior to specifying or ordering any system or equipment. The system and equipment requirements shall be reviewed and agreed as part of the UoE Project T18 consultation process. Technical submittals for all proposed equipment must also be submitted prior to ordering for acceptance by the UoE BSG/Security teams.

3.0 Closed Circuit Television (CCTV) Systems

3.0 Closed Circuit Television (CCTV) System

3.1 General Requirements

All CCTV system design and equipment shall comply with the current edition of BS EN 62676 Parts 1-5, NSI / BSIA guidance and all British/European standards where applicable.

All CCTV equipment shall be **NDAA compliant** to prohibit the use of video surveillance, telecommunications services, equipment and components manufactured by specific vendors in order to quell threats posed to Cyber Security and in turn, security and surveillance.

Please refer to UoE IT Infrastructure Standards V2.2 (August 2019), section 12.0 for CCTV network equipment/cabling to be provided as part of the structured cabling network.

During early RIBA stages, it is the responsibility of the Design Team to liaise with UoE Security via UoE Development Team / BSG to discuss the requirements and performance expectations including operational requirements of associated security system installations, which shall include, and consideration given, but not be limited to the following elements;

- Project overview.
- Project scope of works and associated security measures to be implemented and included within project design.
- Expected security system limitations i.e. budget, building restrictions etc.
- Local Building Control Legislation impact.
- Privacy Impact Assessments.
- Data Protection Act 2018 / GDPR.
- Human Rights Act 1998.
- Freedom of Information Act 2000.
- High risk areas.
- Lone worker/Staff/Student impact.
- Project threat and vulnerability risk assessments.
- Secure by Design considerations.

Due to the complexities, scale and critical nature of protecting both UoE assets and UoE Staff/Students, the security design and installation forms a critical part of the overall project brief and UoE Security Strategy and should be viewed as such.

All CCTV systems shall be of IP based (PoE / PoE+), open protocol technology which meet the requirements of Open Network Video Interface Forum (ONVIF) profiles.

The CCTV system software shall be capable of implementing UoE issued access and password details for each system and individual cameras. Password maintenance to cameras and NVRs must be strictly controlled.

It is possible that in the near future the UoE may migrate its CCTV systems to a cloud-based architecture with virtualised NVR server environments. Therefore, it is essential the design team consider and review this with the UoE Security team during the consultation.

CCTV system software/firmware must be the latest version and fully patched with maintenance cycle supported for minimum of 5 years

The CCTV system should be capable of integrating centralised networked Information stored off site and secure storage off-NVR via an external storage medium (safelocker). Any data must be encrypted in line with best data protection best practice. Any information that is stored remotely or "cloud-based" must be subject to a Data Impact Assessment (DIPA).

UoE Campus CCTV system design shall be compatible and interoperable with the following network recording equipment;

- **UoE Central Area – Geutebrück**
- **UoE King's Buildings Campus - Geutebrück**
- **UoE Easterbush Campus – Avigilon**
- **UoE BioQuarter / Little France Campus – Milestone**

A network video recorder (NVR), based on the manufacturers noted above, shall be included within project design and installed under contract works. It shall be noted that NVR's are not to be omitted under value engineering exercises due to the criticality and purpose this device serves in relation to UoE Security strategies.

NVR memory storage shall be sized to accommodate a minimum of 30 day recorded full HD footage.

NVR's shall be located and housed within the project main communications room, in full agreement with UoE ISG. NVR and all associated CCTV system equipment/cabling, shall be housed within its own separate 42U sized cabinet. Main

comms room and cooling capacity therein, shall be sized adequately and comfortably to accommodate both ISG equipment requirements and CCTV equipment requirements.

Where existing NVRs are being upgraded as part of project works, the decommissioning of these must be agreed with the UoE Security team to ensure secure deletion of images etc. wiped on disposal/decommissioning.

A rack mounted UPS shall be sized and provided within the security cabinet to provide backup power to the CCTV system and network switches for a minimum of 1 hour. This shall be included in the project scope.

Within each cabinet a suitably sized monitor, keyboard/mouse shall be installed to allow local use and permit future modifications.

Cameras shall be wired in CAT6A U/UTP or F/FTP to match the building structured cabling system as a minimum, with 2no, twin data outlets provided at each camera position. CCTV camera connection points shall be installed within each project in such a way to avoid the potential for tampering or disconnection. All associated cabling shall be concealed at both internal and external camera locations. Low level or readily accessible connection points shall not be accepted.

230v power supplies shall be provided at camera locations where/if required.

CCTV camera strategy and connection point locations to be agreed early in the design stage. CCTV cameras shall placed in considered locations so as not to have an over provision of cameras within and around the building. The Electrical designer must consult with UoE Security and UoE BSG to agree provision.

PTZ and/or 4 way+PTZ CCTV cameras shall be strategically mounted externally to monitor the following areas;

- External cycle stores.
- Car park areas (exact coverage to be agreed).
- For use by UoE Security to remotely patrol building and campus locations.
- Externally mounted specialist equipment locations.
- Buildings and surrounding areas that undertake sensitive research.

Static/fixed position CCTV cameras shall where possible, be strategically mounted internally and externally to monitor the following areas;

- All access and egress points of respective building.
- Internal cycle Stores and e-bike charging facilities.

- All interconnecting points to other buildings at each floor level where applicable.
- High risk areas containing cash (inc retail), sensitive UoE Information or valuable assets.
- Vehicle entry barrier locations.
- Loading bay locations.

Note: the use of “fish eye” type cameras is generally prohibited unless specifically agreed with UoE Security team.

Generally all CCTV cameras shall provide overt coverage as a deterrent rather than being covert surveillance.

Pole mounted external CCTV cameras to be provided with raise and lower facility. Poles shall be fitted with all necessary CCTV equipment bracketry and anti-climb guards. CCTV cameras should not be mounted on lighting columns. Camera positions shall take cognisance of the external lighting design to ensure they are not affected by glare etc.

Camera installations of this nature and overall security strategy for site in question shall be agreed with UoE Security / BSG during early design briefings.

CCTV camera mounting heights shall be such that they reduce the likelihood of vandalism or tampering, whilst also recognising the need for future access, maintenance or replacement works that will not require significant access equipment. Final heights shall be agreed on site with UoE Security / BSG.

3.2 CCTV Camera Equipment

As a minimum, CCTV cameras shall meet the performance as described below;

- 5-8MP, 4K / Ultra HD preferred, note the final camera specification to be selected to suit the operational requirements for each camera/area. Exact specification of cameras can be discussed with UoE Security team at design stage.
- High Dynamic Range (HDR).
- 25fps (frames per second) minimum.
- PTZ/ 4 way / static cameras provided to externally monitor perimeter of building.

  c/w optical and digital zoom.
- Static / fixed dome camera provided to internally monitor building access/egress points, connections points to other buildings, public facing areas and retail areas.

- IR LED for low light level use.
- PoE / PoE+.
- Vandal resistant, IK10 minimum dependent on location etc.
- Weather resistant, IP66 minimum dependent on location etc.
- High light compensation (HLC) technology.
- UoE Network Connectivity.
- Open protocol.
- Compression technology.
- Software functionality for motion detection activation (to be agreed with UoE Security team).
- It is not anticipated that Face Recognition or Automatic Number Plate Recognition (ANPR) camera systems will be required on most UoE projects. Should this be required on a specific project due to the sensitivity or location of a project this shall be agreed with the UoE Security team. As a general rule these systems are not approved for use on UoE projects.

3.3 CCTV System – UoE Network Connection

For connection to the UoE Security Hub at Infirmary Street, via the Universities security management system, the Electrical Contractor shall provide media access control addresses (MAC) of all installed camera/recording equipment in order for UoE Security Manager to generate IP addresses not less than 2 months prior to handover. Note all equipment shall be set up for DHCP IP addresses.

UoE Security / BSG shall attend site during CCTV commissioning stage to discuss the system setup and any particular requirements.

Date and time for attendance on site for this shall be agreed with UoE Development Engineer, who will liaise with UoE Security.

3.4 Stand-alone CCTV Systems

On occasion, depending on project and intended use of the building, Academic/End User representatives may request the installation of a stand-alone CCTV system, which is utilised for the sole purpose of monitoring specific types of experiments or research.

These systems do not fall under the management of UoE Security, and unless there is a specific threat to the security of the experiments/research being carried out, do not require connection to the UoE Network for monitoring at UoE Security Central Hub.

In the event monitoring is required by UoE Security, this shall be discussed and agreed between UoE Security and UoE Academic Staff.

The operation and maintenance costs associated with stand-alone systems are departmental and not the responsibility of UoE Security.

Where a standalone system is required by the department/user, these shall be installed, commissioned, and maintained by the UoE incumbent maintenance contractor as the expense of the department.

3.5 CCTV System – UoE T59 Procedure

Under the UoE T59 procedure the Electrical Contractor and their specialist security system contractor will carry out a full demonstration and training of the installed CCTV system.

The UoE Electrical Development Engineer will liaise with the Design/Construction Teams to determine the suitability of the system to ensure it is fully operational prior to demonstrations to UoE Security. When agreed the system is in full operation (including links to UoE Security), a T59 demonstration will be scheduled.

Rack mounted UPS autonomy, and overall system provided for CCTV equipment shall be tested/demonstrated under a mains failure simulation.

The Main/Electrical Contractor will be required to present the following to UoE Security and Development Engineer at the demonstration;

- Complete set of CCTV as installed drawings detailing camera locations, references, data point references and any circuit references where required.
- As installed wiring schematics.
- Asset register of all installed CCTV equipment.
- Maintenance and warranty information of CCTV equipment.
- Equipment/software passwords.
- Keys to CCTV rack.
- Commissioning certificates of CCTV and UPS equipment.

Refer to the project specific T59B/C Document issued by the UoE BSG for full handover and demonstration requirements.

Note as part of the handover as-fitted information, in addition to the general security /CCTV equipment layout, a set of plans and schematic shall be provided that clearly indicates the data network on which the CCTV system operates, these plans shall

show the location of MER/SERs along with patch panels for CCTV systems identified, cable routes and port/outlet numbers associated with CCTV cameras etc.

3.6 CCTV System – Signage

Standard CCTV in operation signage shall be installed within the building at external carpark areas, building entry points and reception. The final locations of CCTV signage shall be agreed with UoE Security team. CCTV Signage shall be included in the project signage package.

3.7 CCTV System – Existing Building Systems

Projects to be undertaken within an existing building, that contain existing CCTV systems shall be assessed by the Electrical Consultant / Contractor in conjunction with UoE Security / BSG to determine existing system requirements or limitations, to ascertain where upgrade works may be required to the support the existing system, ensuring compatibility with new.

4.0 Intruder Alarm Detection System (IADS)

4.0 Intruder Alarm Detection System (IADS)

4.1 General Requirements

All intruder alarm system design and equipment shall comply with the current edition and all relevant parts of PD 6662, BS EN 50131, BS8243 / BS8473, NSI / BSIA guidance and all British/European standards where applicable.

The Electrical Consultant shall include within their electrical specification for the installing security contractor to carry out a risk assessment on the respective building and provide to UoE Security / BSG for review and confirmation of system grade. As a minimum requirement and for tender purposes the Electrical Consultant shall design and specify a grade 3 intruder alarm system.

Whilst UoE Security operate and monitor the Estate 24/7, it is vital that an intruder alarm be provided in buildings intended for 24/7 access and peak hours (08:30-17:30) only, allowing future flexibility for UoE to change use where required.

The intruder alarm equipment provided shall be on a case by case and building basis on a risk assessed approach however, the overall strategy shall be as follows;

- Intruder alarm provided to monitor all external doors and any other potential points of unauthorised entry (identified under the building security risk assessment)
- Motion detection may be required to high-risk areas.
- Motion detection generally required to provide coverage to perimeter ground floor areas to allow the building to be secured when out of use. This shall be the base provision with each project subject to agreement with the UoE Security team.
- Door contacts (including windows where applicable) shall be provided to monitor access/egress during out of normal working hours
- Intruder alarm shall be interfaced to the UoE's iStar system for remote monitoring / alarm activation
- Areas within proposed new and existing buildings that have areas of a sensitive nature, shall be fitted with their own independent intruder alarm which shall also interface to UoE's iStar system for remote monitoring. This approach shall be agreed with UoE Security and Academic End Users only.

4.2 Intruder Alarm Detection System Equipment

The intruder alarm detection system provided shall be fully open protocol and in compliance with the UoE's existing and future maintenance strategy.

The intruder alarm main panel shall be located within the building main electrical switchroom or another location deemed suitable by UoE Security / BSG, location to be agreed on site.

Intruder detection alarm supply shall be fed via 13A unswitched fused connection unit, which shall be engraved in red lettering "INTRUDER ALARM SUPPLY". Supply shall be derived from LV switchroom general power distribution board.

Intruder alarm keypads shall be provided at front entrance and at all other building access doors where required. Keypad location shall be agreed at security strategy design briefing. Additional secondary set/unset KEYPAD shall be included within ground floor plant/switchroom external access doors to avoid need for UoE operations staff to go to reception when out of hours.

Intruder detection alarm equipment shall be provided with the following features as a minimum;

- Main control panel with the following functionality:
    - Multi-zone capability
    - Tamperproof
    - Ethernet module
    - Intruder alarm signal linked to UoE Security via iStar network
    - Panic alarm functionality, critical alarm linked to UoE Security via iStar network
    - GSM capability (for change of use if required)
    - Wireless capability (for future flexibility), all devices hard wired only
    - Open protocol technology
- Keypad – 10no. pre-programmed fob devices shall be supplied
- Door / Window contacts
- Dual technology (Twin Movement) presence detectors with independent signal channels.
- 25% spare capacity provided for future system expansion
- Internal sounder
- External sounder/strobe device, programmed for sounder to switch off after 15 minutes if not reset within this timescale. Strobe shall continue to flash until system is reset.

Siting of the external sounder/strobe on new and existing (and listed) buildings shall be agreed with UoE BSG / Security.

4.3 Panic / Hold Up Alarm

Where the integration of a panic / hold up alarm is required as part of the project requirements, this shall be provided in compliance with the standards stipulated in section 4.2.

The provision of panic alarm systems shall be subject to a risk assessed approach and shall only be provided where there is a significant risk to staff identified.

The request for a panic / hold up alarm including the operation and monitoring of the system shall be discussed at an early stage within the project with UoE BSG / Security and End-User representatives.

Should such a system be provided, this shall be integrated as part of the overall IAD system and monitored via the UoE iStar system by UoE Security. Should there be a requirement to connect to a third party ARC organisation, this shall be agreed with UoE Security. In addition to remote signalling, the panic alarm shall trigger a silent alarm at the intruder alarm panel or local discreet reassurance lamp below the desk.

Panic alarm activation devices shall be wired and securely fixed at public facing locations i.e. reception desks, retail counters and anywhere deemed as a requirement by End-User representatives.

The project will also provide 5no. wireless activation devices for future use as required, and handover to UoE Estates on project completion.

IAD system shall be configured to provide separate critical alarm messages to UoE Security in order to distinguish between unauthorised access and panic / hold up alarm activation.

4.4 Intruder Alarm Detection System – UoE T59 Procedure

Under the UoE T59 procedure the Electrical Contractor and their specialist security system contractor will carry out a full demonstration and training of the installed IAD system.

The UoE Electrical Development Engineer will liaise with the Design/Construction Teams to determine the suitability of the system to ensure it is fully operational prior to demonstrations to UoE Security. When agreed the system is in full operation (including links to UoE Security), a T59 demonstration will be scheduled.

The IAD system and associated panic / hold up system, including critical alarm connection shall be demonstrated to UoE BSG / Security for acceptance.

The Main/Electrical Contractor will be required to present the following to UoE Security and Development Engineer at the demonstration;

- Complete set of IADS as installed drawings detailing main panel, PIR, door/window contacts and keypad locations, including any system data point references and any circuit references where required.
- As installed wiring schematics.
- Asset register of all installed intruder alarm equipment.
- Maintenance and warranty information of intruder alarm equipment.
- Equipment/software passwords.
- Commissioning certificates of intruder and panic / hold up equipment.

Refer to the project specific T59B/C Document issued by the UoE BSG for full handover and demonstration requirements.

5.0 Final Fire Exit Door Monitoring Systems

5.0 Final Fire Exit Door Monitoring Systems

5.1 General Requirements

Unless there has been a specific requirement or risk identified for such a system to be included in the project, the UoE Security Team do not require the inclusion of final exit door monitoring systems.

These systems are not included in, or form part of the UoE Access Control Network.

Should such a system be provided, in agreement with the UoE Security / BSG and End-User representatives it shall not be linked to the building intruder alarm system, but come complete with the capability to do so, should future requirements or changes of use dictate. Standalone system only, if absolutely required.

6.0 Vehicle Barrier and Parking Systems

6.0 Vehicle Barrier and Parking Systems

6.1 General Requirements

Unless there has been a specific requirement or risk identified for such a system to be included in the project, the UoE Security Team do not require the inclusion of vehicle barrier systems on UoE buildings.

Should there be a particular requirement for such a system, whether it be fixed/raise/lower bollards, raise/lower anti-ram ramps or simplistic vehicle barrier entry system this shall be agreed in consultation with UoE Security / BSG / Parking and End-User representatives based on the intended operation of that particular building and associated surrounding site.

Hostile Vehicle Mitigation measures may require to be considered as part of the overall building access strategy. It is essential that for all new major projects that the design team consult with the UoE Security team at an early stage to determine specific requirements and strategy for individual buildings.

6.2 Barrier Equipment

All vehicle barrier installations shall be designed and installed in accordance with the current editions / all parts of PAS 68 and BS6571. Should such a system be provided, it shall be complete with the following operational components and warranties as a minimum;

- Open protocol technology.
- Intercom system and local control of barrier system connected to reception and Building Managers office.
- Access control linked to UoE Network.
- Traffic light system for access/egress.
- Electrical back-up requirements to be discussed during early design stage.
- Emergency fast raise and lower facility, where deemed necessary.
- Manual override and operation.
- Inductive loop system.
- CCTV provided to cover access/egress points.
- Appropriate IP and IK ratings.
- Vehicle impact protection.
- 5-year warranty.
- All BWIC, power supplies, control cabling, data connections, underground ducting etc.

7.0 Appendices

7.0 Appendices

7.1 Appendix No.1: Schedule of Existing Assets

Item	Manufacturer	Description
Access Control Systems	C*CURE 8/9000, iStar etc	Refer to ISG Guidelines. All access control requirements to be discussed with ISG and BSG at design stage
Cabling	BASEC, LPCB and CPR approved manufacturer	As described in EDG No. 6 Electrical Engineering Services and as per security system manufacturers requirements
CCTV	Geutebruck recorder, Milestone (Little France) Avigilon (Easter Bush), Camera Manufacturer (open protocol only, NDAA approved)	Early liaison required on all projects with UoE Security / BSG. First year's maintenance to be included on CCTV system.
Containment	Various manufacturers	As described in EDG No. 6 Electrical Engineering Services
Intruder Alarm Detection System / Panic/Hold Up Alarm	Honeywell Galaxy range or other open protocol manufacturer	First year's maintenance to be included on IADS.
Structured Cabling	Commscope	Refer to ISG Guidelines
UPS	Riello	As described in UPS section of ISG Guidelines

All proposed project equipment and associated manufacturers, including any associated calculation documents shall be provided via technical submittal to UoE Security / BSG for review prior to ordering.

Warranty information shall be provided within O&M documentation on all installed mechanical and electrical equipment, detailing duration (start/end dates), transfer of warranty from purchasing contractor to UoE (if required)

and specific requirements for systems where warranty is dependent on general maintenance.