# Management of security services in higher education

## Security toolchest

The UK Value for Money Steering Group

# Management of security services in higher education: Security toolchest

## Contents

# 1. Purpose and scope of the toolchest

This document and the companion *National report* (HEFCE 2002/30, June 2002) and *Case studies and cameos* (available on the web at www.aucso.org.uk) are the three main outputs from a study of the management of security services in higher education, by the UK Value for Money Steering Group.

The *National report* identifies the key management issues for governors, senior managers and heads of security in developing and reviewing security services, to ensure that they are effective and provide value for money. Important security matters relating to students and staff are also identified. The *Security toolchest* was developed as a practical guide to help higher education institutions (HEIs):

- assess the effectiveness of their security arrangements
- identify matters that need to be considered further
- devise effective solutions
- communicate their policies and procedures for security, personal safety and crime prevention to staff and students.

## Format

The toolchest is divided into 10 elements, ranging from legislation and crime prevention to procurement and staff training. Each element is structured under the following headings:

- Management review objectives. These set out the purpose of the review. HEIs can tailor these to reflect their own concerns more closely, for example by taking objectives from their security service's mission statement or strategy
- Findings from expert working groups**.** A total of 57 institutions contributed to the study through expert working groups. Their conclusions and recommendations are summarised
- Good practice framework, including any issues for smaller HEIs
- Self-assessment checklist and questions
- Cameos from HEIs
- Useful management statistics.

## Using the toolchest

Self-assessment

HEIs can use the tables to carry out an initial assessment of their current security arrangements, and to prioritise areas for improvement. They may then choose to undertake a comprehensive review using the additional self-assessment questions, and the more detailed information in Annex C. In particular, Appendix 2 of Annex C outlines the roles and responsibilities of security staff, in relation to each of the 10 elements of the toolchest.

This assessment will enable the institution to identify and prioritise any management actions required. So that HEIs can draw on existing good practice in the sector, we have provided additional case studies and cameos on the web.

Case studies and cameos from HEIs

The case studies combine the experiences of a number of HEIs, and cover the following broad issues:

- assessing security risks
- developing a security strategy
- training for security staff
- balancing technology and other security measures
- evaluating in-house and contracted-out security provision.

Cameos describe the measures adopted by individual institutions to deal with specific aspects of security. These are listed under each element of the toolchest.

Useful management statistics

The *National report* recommended a strategic approach to security, supported by qualitative and quantitative management statistics to inform decision-making by senior managers, and to help them monitor the effectiveness of policies and procedures. Each element of the toolchest lists useful statistics, as identified by the HEIs that contributed to the study.

## Outcomes and reports to review groups

The results of any reviews could be reported to the institution's appropriate governing committee (such as the audit, estates or health and safety committee), in the form of an annual report and management action plan for consideration and approval. The results could also be communicated to students and staff.

The institution may need to repeat the review periodically to ensure that its arrangements remain effective as circumstances change.

## Further information

Additional information is provided in the bibliography (Annex A), a comprehensive list of references on the web (Annex B), and relevant legislation and good practice guidance (Annex C, Appendix 4).

## 2.1 Security environment

### Management review objectives

- To establish whether the institution has effective management arrangements relating to access by students, staff, visitors and others onto the campus and into buildings.

- To confirm whether the security strategy and related policies require security features to be included in the design of capital projects, and in undertaking minor works (including routine building maintenance).

- To ensure that security features within buildings are appropriate for their intended use by students and staff.

### Findings by expert working groups

Changes in the use of campus buildings have required institutions to adopt new management arrangements for access. This involves assessing risks and considering a range of solutions. In some institutions, existing open access arrangements have been changed to provide more controlled or directed access. Other institutions are increasingly under pressure to open up campus areas and buildings. These facilities are without a manned security presence but are monitored by CCTV, or controlled by automated access systems.

A customer-orientated approach is now required from security staff when responding to the different needs and expectations of external visitors, such as contractors and people attending conferences and cultural events. Some HEIs are considering dedicated pick-up and set-down points for taxis and other vehicles, which may be part of a ‘green’ transport policy for the institution, and also to provide a degree of control of such visitors. The installation of CCTV and improvements to lighting are also important environmental considerations for security services.

Security staff need to be involved at the design and subsequent stages for new buildings and routine minor building works and repairs, to ensure that appropriate security arrangements are installed. These should reflect the proposed use of those areas by students, staff and visitors.

### Good practice framework

- Access cards and passes are issued to students, visitors, suppliers and contractors.

- In agreeing the security access policy the institution invites input from in-house security and safety staff, customers and, if necessary, professional advisers.

- Environmental policies are implemented on, for example, CCTV, lighting, security by design, and transport.

- The institution has established criteria for security by design for key areas of the campus.

Issues for smaller HEIs

- Formulation of a security access policy.
- Implementation of ‘security by design’ principles for identified campus areas and buildings.

## Self-assessment

| Stages within review process | Security environment: checklist | Score (Yes/No)/ Priority (1 to 5) |
|---|---|---|
| **Strategic** | Access policy developed for key campus areas and buildings, integrated within the institution’s security strategic arrangements and its health and safety policies and procedures. | □ □ |
| | Advice sought from head of security in formulating cost-effective policies for security by design for buildings, car parks and campus landscaping. | □ □ |
| | Links created between the security policy and strategy and other environmental policies (for example, the institution’s estate strategy, building maintenance policy, energy policy, and ‘green’ transport strategy). | □ □ |
| | Strategic policy elements of the institution’s security arrangements are in place and regularly updated. | □ □ |
| **Tactical** | Security design criteria established for teaching, research, study, residential, recreational, trading, and student union areas. | □ □ |
| | Access arrangements are incorporated into the security policy and strategy. | □ □ |
| | Security reviews are undertaken promptly for new buildings (pre hand-over) and departmental moves (post-occupancy). | □ □ |
| | Consideration of ‘licensing’ arrangements and establishing ‘pick-up and set-down’ points/areas for contractors, buses, taxis and delivery vans. | □ □ |
| | Security operating procedures annexed/incorporated into the security policy and strategy. | □ □ |
| **Operational** | Security staff and customers consulted during the design stage regarding security measures for new-build and refurbishment projects. | □ □ |
| | Liaison with police architectural design and crime prevention units. | □ □ |
| | Access cards/passes issued to all staff, students, visitors and contractors. | □ □ |
| | All operational security processes and procedures periodically reviewed, in line with changes at strategic and tactical levels. | □ □ |

## Security environment: self-assessment questions

Strategic

1. Are the boundaries of the campus and other areas of the institution, its faculties, schools and departments clearly defined?
2. Is the head of security involved at the design stage for new-build and refurbishment projects, routine maintenance, and departmental moves?
3. Are alarms standardised in accordance with guidelines issued by the head of security?
4. Are locks and keys standardised in accordance with guidelines issued by the head of security?

Tactical

5. Has a security liaison person been appointed for each area within the institution?
6. Has a review been undertaken of entrances and exits to campus buildings, to improve the management of important areas and prevent unauthorised entry?
7. Are visitors encouraged to use the main reception areas of the institution, and are these clearly sign-posted?
8. Are the key (and sensitive) areas of the main buildings covered by the alarm system and other access controls?
9. Are security-related maintenance requests given priority?

Operational

*During working hours*

10. Where necessary:
    - Is it possible to monitor the arrival and departure of visitors?
    - Are visitors asked for identification?
    - Are visitors asked to sign in and out?
    - Are visitors escorted to their destination?
    - Are members of the public prevented from entering restricted parts of the buildings?
11. Do security staff and other members of the institution challenge strangers within buildings and restricted areas?
12. Are fire doors and other emergency exits monitored to prevent unauthorised entry to buildings?
13. Can doors giving access to specific areas be reduced in number without affecting safety? The institution’s safety office should be consulted before the number of doors is reduced.

*Outside working hours*

14. Is external security lighting provided?
15. Is there natural surveillance from surrounding buildings or by passing members of the public?
16. Are there security officers (caretakers/porters or other nominated members of staff) on site 24 hours a day?
17. During shutdown periods, such as at Christmas, does someone co-ordinate a list of people who are authorised to enter the institution, and is a copy provided to security staff?

*Campus*

18. Are the main traffic entrance and exit points linked to CCTV systems?
19. Are entrance and exit barriers raised/lowered manually or automatically (by passes or tokens, for example)? Do the exit barriers lift automatically on approach or is a valid pass/token necessary to raise the barrier?
20. Does the institution have arrangements for maintaining security during construction and for authorising contractors to be on campus premises?

*Off-campus (relations with local residents and businesses, emergency services and other community agencies)*

21. Do security staff represent the institution on local community groups? Do they attend regular meetings with representatives of local authorities, emergency services and other community agencies?
22. Have security staff been assigned responsibilities to act upon issues/activities that impact detrimentally on or near to the campus, such as prostitution, drugs and alcohol abuse, on-street student parking noise disturbance, light pollution, and so on? Are the actions and arrangements to deal with these issues adequately reflected in the institution's policies, as appropriate?

*Buildings*

23. Are the premises in good repair?
24. Are buildings free from examples of flimsy construction, such as low-level glazing or lightweight panelling?
25. Has consideration been given to protecting or eliminating recessed doorways, concealed yards, planted areas and similar features that could give cover to intruders?
26. Have actions been taken to restrict easy access to the roof from points such as adjacent structures, compounds, walls, and drainpipes?
27. Are external and key internal doors locked, and windows and skylights secured, when the premises are not in use?
28. Are tools and ladders locked securely away?

*Alarms*

29. Has an intruder alarm system been installed?
30. Is the alarm installer a member of the British Security Industry Association (BSIA) or the National Approved Council for Security Systems (NACOSS)?
31. Does the intruder alarm system activate lights?
32. Do designated, trained members of staff regulate the alarm system?
33. Is the alarm system regularly maintained and inspected?

*Keys and locking up*

34. Is the locksmith a member of the Master Locksmiths Association, the BSIA or the NACOSS?
35. Is there a system to control the issue of keys?
36. Is there an established procedure for locking up buildings on campus?
37. Are rooms such as toilets and cleaners' cupboards checked to ensure that there is no one concealed in the building when it is secured?
38. Are people who use the building outside normal hours briefed on securing the premises when they leave?

39. Is there a procedure for periodically checking security fittings, such as locks, catches and bolts?

## Cameos from HEIs

Security by design

Access smart cards

Traffic management

## Useful management statistics

Total number of reported incidents for the whole institution for agreed period

Total number of reported incidents (by type, area, time of occurrence) for agreed period

Total number of alarm incidents for the whole institution for agreed period

Total security service coverage per capita, that is, the total number of staff and students divided by the number of dedicated security staff

Perception of personal safety, crime prevention and security (information gathered through surveys)

## 2.2 Legislation, quality and standards

### Management review objectives

- To establish whether the institution has arrangements to ensure that security service standards incorporate agreed customer priorities, existing statutory requirements and good practice guidelines.

- To confirm that the institution properly assesses the implications of statutory requirements and good practice recommendations for its security services.

### Findings of expert working groups

Unlike health and safety, security is not directly covered by legislation, but there are some important legal issues for security staff (and the other services that are managed by them). Relevant legislation is listed in Annex C, Appendix 4, and includes:

Health and Safety at Work (etc) Act 1974

Crime and Disorder Act 1998

Data Protection Act 1998

Working Time Regulations 1998

Fire Safety Act 2000

Freedom of Information Act 2000

Private Security Industry Act 2001

The Crime and Disorder Act 1998 sets out clear responsibilities for local authorities, and there are implications for HEIs because of their position in regional economies and their participation in community partnerships.

Internal legislation, such as the institution's standing instructions, will apply to both internal and external providers of security services. For example, site instructions and supervision arrangements should be provided to external contractors when inviting tenders.

As part of their security arrangements, institutions may wish to implement agreed service level standards that reflect considerations of priority, quality of service, and the continuity of core business activities. The standards could reflect existing legislative requirements and good practice guidance.

### Good practice framework

- Legislation and good practice guidelines have been incorporated in the institution's security policy and security operational manuals.

- Security arrangements enable customers' views to be canvassed and reflected within service level standards/agreements for security services.

- Security arrangements include periodic reviews to confirm that agreed service level standards have been met, and that the assessed levels of security risks and priorities in relation to core business activities were correct.

- Reporting and monitoring systems include management statistics.

Issues for smaller HEIs

- Training arrangements for security staff on changes in legislation related to security services, good practice guidance and European directives.

### Self-assessment

| Stages within review process | Legislation, quality and standards: checklist | Score (Yes/No)/ Priority (1 to 5) |
|---|---|---|
| **Strategic** | Security services mission statements and operating plans are underpinned by service level standards or agreements (SLSs/SLAs). (See Annex C, Appendix 5.) | □ □ |
| | SLSs/SLAs are developed in accordance with 'informed client' best practice. | □ □ |
| | SLAs/SLSs are periodically monitored and updated by the head of security in consultation with client departments. | □ □ |
| | Security services SLAs/SLSs include management statistics that reflect qualitative and quantitative aspects of the operation. | □ □ |
| **Tactical** | Service standards incorporate agreed customer priorities, existing statutory requirements and good practice guidelines. | □ □ |
| | Periodic reviews of compliance with statutory regulations and good practice guidelines are undertaken by security services. | □ □ |
| | The institution and security staff are members of or registered with HE sector organisations and security industry lead bodies such as Association of University Chief Security Officers, Security Industry Training Organisation and Inspectorate of the Security Industry. | □ □ |
| | Security service management statistics reported regularly to governing committees and senior management team. | □ □ |
| **Operational** | Training provided to security staff regarding current and emerging legislation. | □ □ |
| | Codes of conduct identified for all security staff. | □ □ |
| | Operations manual formulated for use by security staff. | □ □ |

### Legislation, quality and standards: self-assessment questions

Strategic

1. What arrangements does the institution have to ensure that it complies with current legislation related to security services? Who is responsible for advising the institution on such matters?

Tactical

2. Does the institution have arrangements for defining and adopting both institutional and departmental service level standards for its security services? (These may be part of its facilities management arrangements.)

Operational

3. Have adequate arrangements been made for the personal safety of staff and employees who work in isolated areas, or with large amounts of cash?
4. If necessary, have guidelines been developed for security staff on how to deal with members of the public exhibiting aggressive behaviour?
5. Are pre-contract meetings held with contractors and other interested parties to identify on-site security, health and safety risks and procedures necessary during the work, including raising alarms and evacuating the site?
6. Is a named person designated to ensure that statutory controls are properly applied and that the appropriate extra security, safety and fire precautions are taken when contractors are working at the institution?

## Cameos from HEIs

Compliance with legislation

## Useful management statistics

Perceptions of personal safety, crime prevention and security (information gathered through surveys)

Incident response times

Total security service coverage per capita, that is, the total number of staff and students divided by the number of dedicated security staff

Ratio of dedicated security service managers and supervisors to security staff

Total number of reported incidents (by type, area, time of occurrence) for agreed period

Total number of alarm incidents for the whole institution for agreed period

## 2.3 Insurance, assessment and management of security risks

### Management review objectives

- To establish how the institution assesses security risks to core activities and key business services.
- To establish how security plans and insurance cover are amended following such assessments.

### Findings of expert working groups

Insurers often act as drivers for risk management, impacting on the risk strategies determined by the institution. The sanctions available to insurers, when the institution does not have appropriate risk management arrangements, are increasing insurance premiums, withholding cover, and raising policy excess thresholds.

Security managers may experience conflicts with insurers over issues involving security and health and safety, fire safety, and other matters. In part, this may arise because of the different groups of assessors responsible for each area.

Effective risk assessment arrangements enable the institution to prioritise limited resources, secure insurance cover at acceptable costs, and balance technological and physical resources for security. The institution's reputation is at risk if it is perceived as an unsafe place.

### Good practice framework

- The institution's security strategy indicates the arrangements and processes by which the assessment of security risks is to be undertaken.
- The assessment of security risks facilitates the updating of operational programmes and financial plans for security services.
- Where in-house staff and/or external advisers undertake an assessment of security risks, the institution ensures that the arrangements and associated processes provide comprehensive and consistent findings.
- Security arrangements include periodic reviews to confirm that the assessed levels of security risk and priority in relation to core business activities were correct, and that agreed service level standards for security services have been met.

Issues for smaller HEIs

- Development of in-house expertise in assessing risk.
- Clear statements of terms and conditions for the appointment of external advisers.

## Self-assessment

| Stages within review process | Insurance, assessment and management of security risks: checklist | Score (Yes/No)/ Priority (1 to 5) |
|---|---|---|
| **Strategic** | Implementation of university-wide ‘business continuity’ arrangements. | □ □ |
| | The institution has considered forming a risk management group to co-ordinate the management of all risks. | □ □ |
| | Head of security is a member of the risk management group. | □ □ |
| | Periodic risk reports are submitted to the governing committees (audit and so on) and senior management team. | □ □ |
| **Tactical** | Definitions for the assessment and prioritisation of security risks are in place and procedures documented. | □ □ |
| | Crime awareness and personal safety guidance published for students, staff and other visitors. | □ □ |
| | Insurance guidelines published, and the head of security is a member of institution’s group for reviewing insurance. | □ □ |
| | Head of security has delegated responsibility for undertaking the assessment of risks and implementing actions identified. | □ □ |
| | Senior management team integrates outcomes of risk assessments for security and for health and safety. | □ □ |
| **Operational** | Insurance register and database of security incidents created. | □ □ |
| | Departmental insurance cover regularly reviewed in consultation with head of security. | □ □ |
| | Security plans and insurance updated by institution following assessments of risks by security staff, as necessary. | □ □ |
| | Insurance policy excesses, claims and losses, incurred by the institution, are monitored and reported to senior management and the head of security. | □ □ |
| | Outcomes of insurance reviews undertaken by insurance providers are discussed with head of security. | □ □ |
| | Details of previous risk assessments and actions implemented are kept by head of security. | □ □ |

## Insurance, assessment and management of risk: self-assessment questions

Strategic

1. Is there a contingency plan to minimise the disruption of normal activities after a serious incident within the institution?
2. What arrangements are in place to ensure that key areas of the campus have been covered by a security survey (or similar form of risk evaluation)?

Tactical

3. How is the assessment of security risks reviewed and revised in accordance with changed circumstances of the institution?

Operational

4. Is there an established procedure for security staff to contact key-holders promptly in the event of serious damage or incidents?
5. Are duplicate records and back-up copies of security computer files kept in a separate location?
6. Do nominated institution staff know their role in an emergency?
7. Are emergency procedures in writing and are they periodically tested and updated?
8. Are the terms and conditions of appointment, scope and approach for the assessment of security risks clearly stated for internal and external assessors?
9. How does the institution ensure consistency in undertaking and analysing the results of such assessments of security risks?
10. Do in-house staff receive appropriate training on the assessment of security risks?
11. How does the institution record the results of the assessment of security risks in a systematic and comprehensive way, to facilitate disseminating management information, updating existing security plans, and confirming or re-assessing the risks and their priority for core business activities?
12. How is the information stored and updated? Is the information costed?

## Cameos from HEIs

Management plans for major emergencies

Reducing false fire alarms

## Useful management statistics

Relationship between losses and claims, that is the total value and number of reported losses of institutional property compared with the total value and number of insurance claims

Total security service coverage per capita, that is, the total number of staff and students divided by the number of dedicated security staff

Total number of reported incidents for the whole institution for agreed period

Total number of reported incidents (by type, area, time of occurrence) for agreed period

## 2.4 Security strategy

### Management review objective

- To establish whether the institution has implemented a strategic and tactical framework for its security services.

### Findings of expert working groups

The institution's security strategy ought to provide links with existing policies, mission statements and service level standards/agreements covering, for example, governance, financial regulations, health and safety, and IT.

Major security incidents affecting the continuity of the institution's core activities will have significant implications. Security services should be represented at a senior level to identify and manage these implications. As part of determining the service arrangements required to address security-related issues, the department responsible for security may wish to develop a mission statement that states the purposes, aims and objectives of the institution's security services. The range of services required may include: safety of personnel and possessions; risk and insurance management; pastoral care; disciplinary matters (both staff and students); and fire, car parking, transport, portering and postal services.

To achieve an effective and co-ordinated approach, the institution may wish to consider implementing an approved security strategy. An outline strategy is included in Annex C, Appendix 1.

### Good practice framework

- A formal, written strategic policy is adopted by the institution that identifies the strategic objectives to be achieved by its security arrangements.

- Effective links are established between the institution's existing academic plans, estates strategy and security plans, to ensure that the objectives for such services are co-ordinated and support other objectives identified by the institution.

Issues for smaller HEIs

- Formulation of a security strategy.
- Establishment of links between the security strategy and other existing strategic and operational documents.
- Consideration of the role and responsibilities of the senior management team (or governing body/resources committee) regarding security arrangements.

### Self-assessment

| Stages within review process | Security strategy: checklist | Score (Yes/No)/ Priority (1 to 5) |
|---|---|---|
| **Strategic** | Security strategy approved and adopted by the institution. | □ □ |
| | Security strategy regularly reviewed by the senior management team, in line with changes in the institution's corporate plan and mission statement. | □ □ |
| | Governing committee advised of changes to security strategy. | □ □ |
| **Tactical** | Links created between the security strategy and other existing strategic policies (for example risk management, IT disaster recovery and data protection policies; university governance and regulations; emergencies and events planning). | □ □ |
| | Role and responsibilities of the senior management team regarding security arrangements are regularly reviewed. | □ □ |
| | Strategic, tactical and operational objectives incorporated in the institution's security strategy. | □ □ |
| **Operational** | Implementation of security strategy reported to senior management team. | □ □ |
| | Annual security report published by the institution. | □ □ |

### Security strategy: self-assessment questions

<u>Strategic</u>

1. Has the institution considered whether security is a key business support service (which may be part of its facilities management arrangements)?
2. What strategic objectives has the institution identified for managing its security arrangements?

<u>Tactical</u>

3. Has the institution incorporated its objectives for security services within its policies and operational plans?
4. Does the institution share its approach to managing security with other HEIs, with a view to learning from each other?

Operational

5. Does the institution have arrangements to fulfil the ‘informed client function’ for its security services?

6. If there is a security strategy, is it:

- documented and formally adopted by the institution? If YES, when was it last reviewed and who approved it?
- written, but not approved? If YES, when was it produced and who has agreed it?
- an unwritten set of guidelines? If YES, is it implicitly contained in other existing strategic policy documents?

7. What plans and processes does the institution have to support the delivery of its security strategy (such as surveys to assess risk, security programmes, budgets and financial planning, management information systems, and service level standards)?

## Cameos from HEIs

Reviewing the security strategy

Policies and procedures put into practice

Management responsibility for security services

Total reorganisation – introduction of dedicated security staff

## Useful management statistics

Perception of personal safety, crime prevention and security (information gathered through surveys)

Ratio of dedicated security service managers and supervisors to security staff

Total security service coverage per capita, that is, the total number of staff and students divided by the number of dedicated security staff

Incident response times

Number of logged contacts and incidents by the security office or control centre for agreed period

Total number of reported incidents (by type, area, time of occurrence) for agreed period

Number of written complaints and compliments to security services received per agreed period (in-house and contract staff)

## 2.5 Security management structures and links with other services

### Management review objective

- To establish whether the institution has effective management arrangements for co-ordinating and undertaking security services; and how they interconnect with other support services.

### Findings of expert working groups

Management for security services varies considerably between HEIs. As part of a review process, institutions may need to consider whether the management of security is in the best place. Some situations dealt with by security can and do have serious implications for institutions. Therefore managers responsible for security need to be able to consult quickly with other senior managers, and to co-ordinate actions with external agencies. Representation at senior management level is an important part of the solution. Whoever has ultimate responsibility for security needs a wide range of management skills.

The institution has a choice in the mix of contracted internal and external security services. Effective arrangements should combine flexibility, to respond to changing needs, with cost-effectiveness, whereby resources are committed on the basis of management and staff skill requirements, linked to agreed service standards.

### Good practice framework

- Provision of management, staff and professional services is based on an agreed service level requirement and is subject to periodic reviews.

- Identifying component costs within security services helps to assess the performance and cost-effectiveness of existing arrangements.

- Staff and management training arrangements ensure that security services may be carried out safely, comply with legislation, and deliver value for money to the institution.

<u>Issues for smaller HEIs</u>

- Co-ordination of security and other support services.

## Self-assessment

| **Stages within review process** | **Security management structures and links with other services: checklist** | **Score (Yes/No)/ Priority (1 to 5)** |
|---|---|---|
| **Strategic** | Management structure reviewed by the institution to ensure the delivery of the objectives in its security strategy. | □ □ |
| | Security services departmental mission statements and operating plans in place. | □ □ |
| | Senior manager identified with responsibility for security. | □ □ |
| **Tactical** | Policies developed regarding specific measures to support the institution's security strategy. | □ □ |
| | Strategic and tactical responsibilities for security established within the senior management team. | □ □ |
| | Links to other support services identified as part of an integrated approach to services and risk management. | □ □ |
| | Head of security appointed. | □ □ |
| | Review of security and related services undertaken using the *Guidance on the procurement of services* (Joint Procurement Policy and Strategy Group, Volumes 1 and 2, September 2000). | □ □ |
| **Operational** | Dedicated security staff appointed. | □ □ |
| | Departmental and security liaison representatives appointed. | □ □ |
| | Security staff job descriptions and organisational charts updated. | □ □ |
| | Routine security checks introduced, and duties to be undertaken by non-security staff and students considered. | □ □ |

## Security management structures and links to other services: self-assessment questions

Strategic

1. Does the management structure of the security services support the delivery of the institution's corporate business plan?
2. Have the strategic, tactical and operational requirements for the security services been identified?

Tactical

3. Has the institution identified the stakeholders for its security services and the arrangements for determining their service needs?
4. Are security services subject to service level agreements or statements, and do service plans indicate the required strategic, tactical and operational objectives to be achieved?

Operational

5. Are stakeholders formally consulted on their current and future security service needs?

6. Does the institution consider the following issues for security services , whether provided internally or externally (both individually and on a group basis):

    - provision/availability of closely-related services?
    - existing/potential areas of overlap in providing security services?
    - integration/co-ordination between other support services and existing security services?
    - measurement and evaluation of stakeholders' perceptions of value for money regarding its security services (which may be as part of its facilities management arrangements)?

7. Has the institution appointed a dedicated security manager? If other arrangements apply, what are they? Does the manager responsible have the appropriate professional skills and time to act effectively in the management of its security services?

8. Are some management responsibilities for security delegated to other service providers? How are the overall arrangements for security services co-ordinated?

9. What actions have been taken by security staff regarding liaison with customer departments, the dissemination of management information, and so on?

## Cameos from HEIs

Security audits

Incident management

Combined security and postal services

Rotation of security staff roles

Liaison with other departments

## Useful management statistics

Total security service coverage per capita, that is, the total number of staff and students divided by the number of dedicated security staff

Ratio of dedicated security service managers and supervisors to security staff

Percentage staff turnover, that is, total resignations per annum divided by total number of security staff

Number of written complaints and compliments received by security services per agreed period (in-house and contract staff)

Number of contacts and incidents logged by the security office/control centre for agreed period

Total number of reported incidents (by type, area, time of occurrence) for agreed period

## 2.6 Raising awareness of crime, and crime prevention

### Management review objective

- To establish whether the institution has arrangements to promote personal safety, security and crime prevention among students, staff and visitors.

### Findings of expert working groups

In the early stages of the study, it was apparent that a number of HEIs had been proactive in developing collaborative partnerships, both within and outside the institution. This is an important part of providing effective security services for the benefit of students, staff and visitors, and contributes to the reputation of the institution within local, national and international communities.

The perception of crime by staff and students is an important issue. One approach to allay the fears of staff and students and to engender a ‘feel-good’ factor is to develop partnerships with local agencies, such as the police and local authorities. Adoption of a multi-agency approach has proved successful in securing a safe environment on and off campus. The Crime and Disorder Act 1998 places a responsibility on local authorities to work with other organisations – including HEIs – in tackling crime.

### Good practice framework

- Adoption of a multi-agency approach.
- Development of local partnerships within the community.
- Security arrangements take account of customers’ views and reflect these within service delivery statements.

Issues for smaller HEIs

- Use of customer satisfaction surveys.
- Liaison arrangements for security services.

## Self-assessment

| Stages within review process | Raising awareness of crime, and crime prevention: checklist | Score (Yes/No)/ Priority (1 to 5) | |
|---|---|---|---|
| **Strategic** | Security awareness strategy implemented for students, staff and visitors. | □ | □ |
| | Multi-agency approach to crime prevention adopted by the institution. | □ | □ |
| | Security performance reviewed to identify areas/actions for further improvements. | □ | □ |
| | Annual security report published. | □ | □ |
| **Tactical** | Key groups of people identified that could support and/or contribute to security initiatives. | □ | □ |
| | Institution is represented on key community groups. | □ | □ |
| | Personal safety and crime awareness/prevention material is available to students and staff and is reviewed periodically. | □ | □ |
| | Head of security is responsible for evaluating security initiatives regularly. | □ | □ |
| | Management information provided to senior management team on security is regularly reviewed. | □ | □ |
| **Operational** | Roles and liaison arrangements with staff and student unions established. | □ | □ |
| | Periodic advice and consultation provided for students as part of 'Freshers week', and for new staff at induction meetings. | □ | □ |
| | The head of security holds regular meetings with heads of academic and other service departments. | □ | □ |
| | Student and staff satisfaction surveys undertaken on, for example, security awareness and effectiveness of crime prevention information. | □ | □ |

## Raising awareness of crime, and crime prevention: self-assessment questions

Strategic

1. Does the institution promote personal security and safety issues for students, staff and visitors?
2. Are staff and students reminded of personal security responsibilities at the start of each academic year?

Tactical

3. Has the head of security undertaken a risk evaluation survey of the institution's premises (both on and off campus), and have the recommendations been implemented?

Operational

4. Is the institution involved in multi-agency partnerships and are security arrangements covered in these?
5. Does the institution periodically seek advice – on up-to-date security technology, crime prevention measures and damage control – from the police crime prevention and architectural liaison officers, other HEIs, and organisations within the security industry?
6. Has the institution implemented Home Office security-related initiatives?
7. Is the institution a member of National Crimestoppers UK and regional and local crime prevention groups?
8. Is the institution in contact with other businesses in the area/region to exchange information about security?
9. Is the institution aware of relevant crime and security-related initiatives introduced by the local authority?
10. Are there 'campus watch' schemes for residential and non-residential areas?
11. Has guidance been sought from the security department on crime prevention measures and damage control?
12. Does the institution conduct workshops and other meetings to help stakeholders think about their future security service needs (which may be part of its facilities management arrangements)?
13. What arrangements are there to undertake customer satisfaction surveys regarding security services?

## Cameos from HEIs

Establishing communication and partnerships

Links with the local police

Rapport with local communities and local councils

Multi-agency approach

Emergency response teams

Campus watch schemes

Local early warning systems

Student security groups – students and staff

Emergency telephone numbers

Crime prevention publications

Personal safety

Student surveys

Security services web pages

## Useful management statistics

Perception of personal safety, crime prevention and security (information gathered through surveys)

Total security service coverage per capita, that is, the total number of staff and students divided by the number of dedicated security staff

Incident response times

Number of contacts and incidents logged by the security office or control centre for agreed period

Total number of reported incidents (by type, area, time of occurrence) for agreed period

## 2.7 Procurement

### Management review objective

- To establish whether the institution assesses the cost-competitiveness of security services against market conditions (whether undertaken internally, by externally contracted service providers, or by a mixture of the two), as part of satisfying agreed standards for service delivery.

### Findings of expert working groups

Effective procurement and costing can help the institution to achieve value for money through identifying security requirements, managing contractual arrangements, undertaking contract reviews, assessing contractor/consultant performance, and carrying out market-based cost comparisons.

Purchasing arrangements for security services should be supported by appropriate sections within the institution's Financial Regulations, and comply with EU legislation.

### Good practice framework

- Procurement arrangements demonstrate that value for money can be delivered for agreed levels of service delivery for security services.
- Procurement arrangements for agreed security needs can be consolidated, to achieve economies of scale for the institution and individual departments.
- Computerised procurement systems facilitate the reporting and management of security contracts; and support periodic management reviews of service, cost, delivery and performance.
- Procurement arrangements for security equipment and services are documented, and comply with UK and EU legislation.

Issues for smaller HEIs

- Review of purchasing and contract arrangements.
- Assessment of contracts and costs against market conditions.

### Self-assessment

| Stages within review process | Procurement: checklist | Score (Yes/No)/ Priority (1 to 5) |
|---|---|---|
| **Strategic** | Security service contracts and purchasing arrangements allow the institution to respond to market conditions. | □ □ |
| | Tendering and financial regulation procedures are updated periodically. | □ □ |
| **Tactical** | Roles and liaison arrangements have been identified for negotiating and monitoring security service contracts, between security and purchasing staff. | □ □ |
| | Review of security services procurement is undertaken using the *Guidance on the procurement of services* (Joint Procurement Policy and Strategy Group, Volumes 1 and 2, September 2000). | □ □ |
| **Operational** | Procurement arrangements for security services comply with UK and EU legislation. | □ □ |
| | Security procurement arrangements and services are periodically subjected to market testing and other reviews to assess value for money. | □ □ |

### Procurement : self-assessment questions

Strategic

1. Does the institution have an appropriate procurement strategy for its security services?

Tactical

2. Are there service standards for internal and external service providers of security services?
3. Are there up-to-date specifications for security services, whether provided internally or externally?
4. Does the institution have arrangements to determine how its security services – both internal and external – are to be provided? (These may be part of its facilities management arrangements.)
5. Does the institution undertake periodic reviews of its security service arrangements, both internal and external, involving one or more of the following processes:
    - market testing (formal and soft)?
    - departmental (faculty/school) reviews?
    - stakeholder service reviews?
    - contract reviews with service providers?
6. Are there explicit procurement procedures for security services and supplies, whether provided internally or externally?
7. Does the institution have tendering arrangements for externally provided security services and supplies, above specified contract values?

Operational

8. Are there procedures to investigate complaints by stakeholders about delivery of security services?
9. Has the institution formed co-operative relationships with its security service providers?
10. Does the institution review service level standards/agreements with its security service providers and stakeholders?
11. How often are the security contract terms and costs reviewed?
12. Who provides advice to the institution on purchasing, contracting, and opportunities for security services and supplies?
13. Is there a list of approved security contractors and consultants? If so, how is it kept updated?
14. Does the institution use standard contract forms for its security services?
15. How is a short-list of potential suppliers for security services and supplies drawn up, and who is involved? Does the institution carry out post-tender negotiations?
16. How does the institution ensure that the purchasing and contracting arrangements for security services and supplies comply with its Financial Regulations?
17. Do the purchasing and contracting arrangements comply with EU legislation?

## Cameos from HEIs

Combined in-house and contracted security services

In-house security staff

Community safety partnerships

Funded police officers

Relations with police

## Useful management statistics

Incident response times

Ratio of dedicated security service managers and supervisors to security staff

Percentage staff turnover, that is, total resignations per annum divided by number of security staff

Average period of sick leave per person: that is, number of days per annum of self-certificated sick leave divided by total number of security staff

Total number of training days received per member of security staff (in-house and contracted) over an agreed period

Total number of training days delivered per member of security staff (in-house and contracted) over an agreed period

## 2.8 Staff training and development

### Management review objective

- To establish whether the institution has effective management arrangements for co-ordinating and undertaking training and development of security staff.

### Findings of expert working groups

Institutions as employers have responsibilities under the Health and Safety at Work etc Act 1974 that can be met by providing effective training arrangements. The Data Protection Act 1998 has implications for training security staff in data management and the use of surveillance systems.

Students, staff and visitors (as customers) have specific expectations regarding the delivery of security services. A number of HEIs have undertaken customer surveys to establish the exact nature of the services required, and the management statistics to be collected to confirm the effectiveness of the arrangements.

Resources are limited, and the institution's staff need to be flexible in meeting the service demands; training arrangements can help them do so. Good systems for induction and training can provide an incentive to existing and prospective staff by confirming the value of their role.

### Good practice framework

- Staff and management training arrangements are in place so that security services can be carried out safely, comply with legislation, and deliver value for money. For further details please see *Rewarding and developing staff in higher education: a guide to good practice in setting HR strategies* (HEFCE 02/14, March 2002).

Issues for smaller HEIs

- Review of security staff induction and training arrangements.
- Development of management skills relating to the assessment of security contracts.

## Self-assessment

| Stages within review process | Staff training and development: checklist | Score (Yes/No)/ Priority (1 to 5) |
|---|---|---|
| **Strategic** | Training policies for security staff are in place. | □ □ |
| | Personal development plans and staff appraisal procedures are in place for security staff at departmental and individual levels. | □ □ |
| | Central and departmental funding of training initiatives is subject to periodic review. | □ □ |
| | Recommendations on training by the Association of University Chief Security Officers (AUCSO) are considered by the institution and implemented where appropriate. | □ □ |
| **Tactical** | Security staff training arrangements are linked to national training objectives such as promoted by AUCSO and the Security Industry Training Organisation (SITO). | □ □ |
| | Core competencies identified for all security staff and included in job descriptions and staff appraisal processes. | □ □ |
| | Skills audit of security staff periodically undertaken. | □ □ |
| **Operational** | List of core training courses developed for all levels of security staff. | □ □ |
| | Structured induction sessions provided for new security staff. | □ □ |
| | Training programmes created for existing security staff. | □ □ |
| | Training programmes regularly reviewed. | □ □ |
| | Feedback from training events provided to other security staff, and security issues/implications summarised for institution. | □ □ |

## Staff training and development: self-assessment questions

Strategic

1. Are there arrangements to audit staff skills (to identify areas of expertise/gaps in skills) and thereby determine the institution’s management needs with regard to key security services?

Tactical

2. Does the institution enable security services staff to undertake appropriate qualifications in security and facilities management?
3. Does the institution enable security services staff to undertake continuing professional development and to develop their experience?

Operational

4. Are institution staff warned to notify security of suspicious activities or suspicious strangers on the institution’s premises?

5. Do new security staff (including contract security staff) receive appropriate induction training regarding their duties and responsibilities in relation to the institution and its membership (students, staff and visitors)?
6. Do security staff have a personal training and development programme?
7. Are the terms and conditions of employment for security staff subject to review?
8. Do security staff undertake annual medical checks? What arrangements are in place if the required physical fitness/health levels are not reached – for example, can security staff be re-deployed?
9. What arrangements does the institution have for keeping security staff updated about security matters (for example, by providing training, or subscribing to professional journals)? How regularly are these arrangements reviewed?

## Cameos from HEIs

Induction training and personal development courses

Investing in continuing professional development

Dedicated in-house training

Comprehensive training and development programme

Instruction manual for security staff

## Useful management statistics

Ratio of dedicated security service managers and supervisors to security staff

Number of training days delivered over a period per member of security staff (in-house and contracted)

Number of training days received over a period per member of security staff (in-house and contracted)

Number of reported incidents for the whole institution for agreed period

Total number of reported incidents (by type, area, time of occurrence) for agreed period

Number of alarm incidents for the whole institution for agreed period

Number of incidents captured on CCTV for the whole institution for agreed period

Incident response times

## 2.9 Balancing technology with other security measures and resources

### Management review objectives

- To establish whether the institution has appropriate management arrangements regarding the use of existing and emerging technology, such as CCTV and control systems, and security equipment.
- To confirm whether effective arrangements are in place regarding staffing and other resources.
- To improve the value for money from funds invested in security initiatives.

### Findings of expert working groups

Solutions to security issues are increasingly being linked to technology, but these often have wider implications. For example, security incidents captured on CCTV equipment require an operator to monitor and initiate action. Similarly, preparing operational plans, creating asset registers, and co-ordinating different systems may require technological, staffing and other resources. A consideration for a number of institutions is ‘getting the balance right’.

Security planning can save money for institutions if there are effective processes to identify security requirements; to assess risk and priority in relation to core business activities; to co-ordinate capital and revenue security programmes; and to monitor security services.

### Good practice framework

- Planning systems, such as computerised databases (or spreadsheets), facilitate updating and manipulation of data following an assessment of risk and the reassessment of security priorities.
- Operational security programmes are costed to identify the financial resource requirements.

Issues for smaller HEIs

- Introduction of operational security programmes.

### Self-assessment

| Stages within review process | Balancing technology with other security measures and resources: checklist | Score (Yes/No)/ Priority (1 to 5) |
|---|---|---|
| **Strategic** | Policies have been developed by the head of security for the operation of manned guarding and dog patrols; use of CCTV, alarms and other physical access controls; and the integration and standardisation of security systems and locks and replacement of keys. | □ □ |
| | Allocations of resources are regularly reviewed by the senior management team in line with changes in institution's security strategy. | □ □ |
| **Tactical** | Life-cycle periods and criteria for repair or replacement have been agreed for security control systems and equipment. | □ □ |
| | Asset and insurance registers are integrated to support security management. | □ □ |
| | Integrated control systems and monitoring mechanisms established for equipment associated with security, fire, safety and energy. | □ □ |
| **Operational** | Security and installed services data are collated from estate records, 'as-built' plans, service manuals and so on to support security management. | □ □ |

### Balancing technology with other security measures and resources: self-assessment questions

Strategic

1. Does the institution consider whole-life costs in implementing security arrangements?
2. Are there security programmes and plans for each campus?

Tactical

3. Are security plans and schedules developed on the basis of the institution's security priorities?
4. How are the operational plans updated following periodic assessment of risks?

Operational

5. Are there secure storerooms or containers for valuable items such as audio-visual equipment, computers and videos?
6. Are rooms containing other valuable equipment - offices, workshops and storerooms – kept locked when not in use?
7. Are staff and employees advised on the need to safeguard property?
8. Are secure worktop fittings provided for valuable portable equipment?
9. Are cash holdings kept to a minimum?
10. Is cash counted out of sight of potential thieves?
11. Is money removed from the premises overnight?

12. Who undertakes cash movement – internal or external? Staff or security services?
13. Are special arrangements in place, such as the issue of personal attack alarms, to protect vulnerable staff?
14. Is equipment marked to identify the owner (for example, as the institution or an individual member of staff or a student), and are signs displayed to this effect to deter thieves?
15. Have special arrangements been made to protect items of particular interest to thieves, such as large food stocks, shop supplies, tools, solvents and drugs?
16. Are equipment cartons disposed of promptly and discreetly to avoid alerting potential criminals?
17. Are expensive items of equipment located away from ground floor windows and doors?
18. Are high value items, such as digital projectors and computers protected by dedicated alarm systems?
19. Are car parks and bicycle sheds assessed for risk of vandalism and theft, and appropriate crime prevention measures implemented (such as adequate lighting, CCTV and regular security patrols)?
20. Are staff and students provided with guidance to minimise the loss of personal possessions?
21. Does the intruder alarm automatically notify security staff via a central control room?
22. What links exist between security and other emergency systems?
23. Are asset registers kept for security equipment?
24. How are 'as-built' drawings and security manuals prepared, stored and updated for security equipment and systems?

## Cameos from HEIs

Linked CCTV and card access systems

Individual intruder alarms linked by auto dialling to control room

Personal safety and security measures

Window grilles and alarm contacts on doors

Campus patrols – security duties for non-dedicated security staff

Monitoring security patrols

Manned and dog patrols

Use of security vehicles

Operational procedures manual

## Useful management statistics

Incident response times

Number of logged contacts and incidents by the security office or control centre for agreed period

Number of incidents recorded on CCTV for the whole institution for agreed period

Number of alarm incidents for the whole institution for agreed period

Total number of reported incidents (by type, area, time of occurrence) for agreed period

Number of reported incidents for the whole institution for agreed period

## 2.10 Funding and service performance

### Management review objective

- To establish whether the institution is able to fund the delivery of security services, based on an assessment of risk to the institution and its activities. The actions necessary ought to be prioritised, and disclosed in the strategic, tactical and operational plans for security.

### Findings of expert working groups

To develop effective security arrangements, funding requirements should be identified in strategic, tactical and operational plans. The level of funding ought to take account of agreed priorities determined by a robust assessment of risk, and should deliver the defined levels of service standards. In particular, the personal safety of students, staff and visitors will be an over-riding concern. Funding that is based exclusively on past experience will provide only partial solutions.

### Good practice framework

- Funded and standards-led levels of service delivery are established for security arrangements.

- Budgets are based on co-ordinated and costed security plans and programmes.

- The implications of deferring or not funding security services can be ascertained, using life-cycle cost-in-use techniques. For further details please see *Whole life costing: a good practice guide* (Joint Procurement Policy and Strategy Group, August 1998).

- Computerised financial planning systems in the security department can help staff to:
  - update and manipulate data following the assessment of risk
  - confirm and reassess security priorities and other planned changes
  - make data compatible with and transferable to other systems, as necessary.

- Reporting and monitoring systems include management statistics for security services, and the identification of life-cycle costs funded by security-related capital and revenue expenditure.

- The review and monitoring process is based upon reported performance against quality, quantity, time and price.

<u>Issues for smaller HEIs</u>

- Security plans and programmes.
- Identification of management statistics.
- Review of budget arrangements for security services.

### Self-assessment

| **Stages within review process** | **Funding and service performance** | **Score (Yes/No)/ Priority (1 to 5)** |
|---|---|---|
| **Strategic** | Financial appraisal arrangements reviewed to assess value for money for security initiatives. | □ □ |
| | Funding of security services linked to service level standards/agreements. | □ □ |
| | The institution exchanges security management statistics with other institutions for their mutual benefit. | □ □ |
| **Tactical** | Investment criteria, appraisal methods, monitoring and documentation are in place for security initiatives. | □ □ |
| | The assessment of security initiatives includes the identification of cost-benefits. | □ □ |
| | Finance, asset and space management systems are integrated with the security management information system (SMIS). | □ □ |
| | SMIS provides historic data to monitor progress and to extrapolate trends in security incidents. | □ □ |
| **Operational** | SMIS reviewed to ensure that effective management information and statistics are produced for the senior management team. | □ □ |
| | The management statistics are regularly reported to the institution's senior management. | □ □ |

### Funding and service performance: self-assessment questions

Strategic

1. Is the contribution made by the security services reported in the institution's corporate business plan?
2. Are there appropriate planning and review arrangements for the delivery of security as a key support service?
3. If security budgets are devolved to academic and administrative departments, what arrangements are in place to ensure that the security services priorities identified are funded and undertaken in compliance with legislation?
4. Has the institution developed long-term financial models and forecasts for its security services?
5. What are the arrangements at institutional, faculty, school and departmental levels to act on, monitor and report criminal, fire, health and safety and other risk-related incidents? These include management information systems, procedures and processes.

Tactical

6. What are the arrangements at institutional, faculty, school and departmental levels to identify the total cost of burglary and theft, assault, and criminal damage?
7. Has action been taken to deal with any areas that have been identified as particularly vulnerable to vandalism or forced entry?
8. Has there been any deferment of expenditure on crime or fire prevention measures?

Operational

9. Has any money been specifically allocated for the prevention of crime and vandalism over the next five years?

10. Does the institution identify both direct and indirect costs of providing security services to faculties, departments and so on?

11. Does the institution identify the cost of managing internal security services?

12. Are charges to faculties and departments, for the allocation of security services costs, kept under review?

13. Does the institution determine its security service budgets:

    - from first principles by adopting zero-based budgeting?
    - by prioritising relevant stakeholders' needs?

14. Do information systems provide an up-to-date picture of committed and likely future security service costs for relevant stakeholders?

15. Are service level agreements/statements (SLAs/SLSs) and service specifications/contracts subject to annual and other periodic service reviews?

16. Are there management statistics for security services, as part of demonstrating value for money?

17. Does the institution measure the performance of security service providers, both in-house and contracted out?

18. Is security service performance monitored and reported to senior management and stakeholders regularly?

19. Does the institution benchmark the costs of its security services against those of other institutions/organisations within and outside the HE sector?

20. Are the comparisons of security costs with the budgets communicated to departments on a regular basis?

## Cameos from HEIs

Monitoring crime statistics to target resources

Allowing 10% of property value to provide effective security measures

Devolving of security budgets to head of security

Income generation: extending security services to local businesses

## Useful management statistics

Costs of implementing legislation related to security

Ratio of dedicated security service managers and supervisors to security staff

Percentage staff turnover, that is, total resignations per annum divided by number of security staff

Average period of sick leave per person: that is, number of days per annum of self-certificated sick leave divided by total number of security staff

Incident response times

Number of reported incidents for the whole institution for agreed period

Number of training days delivered over an agreed period per member of security staff (in-house and contracted)

Number of training days received over an agreed period per member of security staff (in-house and contracted)

# Annex A Bibliography

‘Appraising investment decisions’ (HEFCE 99/21)

‘Facilities management: improving the management of support services in higher education’ (National Report, HEFCE 00/14)

‘Guidance on the procurement of services’ (Joint Procurement Policy and Strategy Group (Volumes 1 and 2, September 2000)

‘Handbook of security’ (Kluwer - Volumes I and II, Croner CCH Group Ltd, 2001)

‘Legal services: a guidance note for institutions’ (Association of Heads of University Administration, April 2000)

‘Management information for decision making: costing guidelines for higher education institutions’ (HEFCE M13/97, July 1997)

‘Policing the campus’ (Strathclyde Constabulary, 1998)

‘Premises management - practical premises security’ (Croner CCH Group Ltd, 2001)

‘Research Briefings 1999/2000 Series’ (Association of British Insurers, 2001)

- Crime statistics underwriting – burglary
- Effectiveness of CCTV
- Future crime trends in the UK
- Intruder alarms signalling

‘Rewarding and developing staff in higher education: a guide to good practice in setting HR strategies’ (HEFCE 02/14)

‘Risk management – a briefing for governors and senior managers’ (HEFCE 01/24) and ‘Risk management – a guide to good practice for higher education institutions’ (HEFCE 01/28)

‘Strategic planning in higher education – a guide for heads of institutions, senior managers and members of governing bodies’ (HEFCE 00/24)

‘Student living report 2002’ (UNITE) www.unite-group.co.uk

‘Whole life costing: a good practice guide’ (Joint Procurement Policy and Strategy Group, August 1998)

# Annex B Useful references

The following are useful references for HEIs. This does not imply any recommendation by the higher education funding bodies.

## Higher education funding bodies and sector organisations

**Higher Education Funding Council for England (HEFCE)**
www.hefce.ac.uk

**Higher Education Funding Council for Wales (HEFCW)**
www.wfc.ac.uk/hefcw

**Higher Education Staff Development Agency (HESDA)**
www.hesda.org.uk

**Scottish Higher Education Funding Council (SHEFC)**
www.shefc.ac.uk

**Standing Conference of Principals (SCOP)**
www.scop.ac.uk

**Universities Scotland (formerly COSHEP)**
www.universities-scotland.ac.uk

**Universities UK (formerly CVCP)**
www.universitiesuk.ac.uk

## HE discussion groups, management services and steering groups

**Academic Institutions Management Services (AIMS)**
www.aims.ac.uk

**Association of University Chief Security Officers (AUCSO)**
www.aucso.org.uk

**Association of University Directors of Estates (AUDE)**
*Scottish Association of University Directors of Estates (SAUDE)*
*Higher Education Directors of Estates for Wales (HEDEW)*
www.heestates.ac.uk/Partners/AUDE

**Higher education estates web-site**
www.heestates.ac.uk

**Joint Costing and Pricing Steering Group**
www.jcpsg.ac.uk

**Joint Procurement Policy and Strategy Group**
www.jppsg.ac.uk

**Police Association of Higher Education Liaison Officers (PAHELO)**
www.soton.ac.uk/~pahelo

**Southern Universities Management Services (SUMS)**
www.sums.org.uk

## Security-related organisations

**Association of British Insurers (ABI)**
www.abi.org.uk

**Association of Security Consultants (ASC)**
www.securityconsultants.org.uk

**British Security Industry Association (BSIA)**
www.bsia.co.uk

**European Association of Campus Security (EACS)**
www.euro-campus-secur.org

**Inspectorate of the Security Industry (ISI)** *(now part of the National Security Inspectorate)*
www.isi.org.uk

**Institute for Supervision and Management (ISM)**
http://www.trainingzone.co.uk/ism

**International Association of Campus Law Enforcement Administrators (IACLEA)**
www.iaclea.org

**International Institute of Security (II Sec)**
http://www.iisec.co.uk

**International Professional Security Association (IPSA)**
www.ipsa.co.uk.com

**Joint Security Industry Council (JSIC)**
www.jsic.co.uk

**Master Locksmiths Association**
http://www.locksmiths.co.uk

**National Approval Council for Security Systems (NACOSS)** *(now part of the National Security Inspectorate)*
www.nacoss.org

**National Examining Board for Supervision and Management (NEBSM)**
http://www.olc.ccta.ac.uk/nebsm.htm
*Refer also to NEBS Management*
http://www.nebsmgt.co.uk

**National Security Inspectorate (NSI)**
www.nsi.org.uk

**Security Industry Training Organisation (SITO)**
www.sito.co.uk

**Security Institute of Ireland**
http://www.sii.ie/welome_to_the_security_institute.htm

**Security Systems and Alarms Inspection Board (SSAIB)**
www.ssaib.co.uk

## Security news, directories, publications and other on-line resources

**Acts of Parliament**
www.hmso.gov.uk/acts.htm
*Refer also to Government documents*
*www.hmso.gov.uk and www.official-documents.co.uk*

**Association of Chief Police Officers of England, Wales and Northern Ireland**
www.acpo.police.uk

**Association of Local Authority Risk Managers (ALARM)**
www.alarm-uk.com

**Building Research Establishment (BRE) Certification Division**
www.brecertification.co.uk

**BRE Fire and Risk Sciences Division**
www.bre.co.uk/frs

**British Standards Institution**
www.bsi.org.uk

**Crime Concern Trust Limited**
www.crimeconcern.org.uk

**Crime prevention**
www.homeoffice.gov.uk/crimprev/cpindex.htm

**Crime reduction**
www.crimereduction.gov.uk
*Refer also to Policing and Crime Reduction Group*
http://www.homeoffice.gov.uk/pcrg/index.htm

**Crimestoppers Trust**
www.crimestoppers-uk.org

**Fire, health and safety, and security (web portal)**
www.uprotectit.com

**Fire safety**
www.fire.org.uk
*Refer also to Arson Prevention Bureau*
www.arsonpreventionbureau.org.uk

**Government documents and other official publications**
www.hmso.gov.uk
www.official-documents.co.uk
*Refer also to Acts of parliament*
www.hmso.gov.uk/acts.htm

**Health and Safety Executive**
www.hse.gov.uk

**Health and safety information**
www.safety-directory.co.uk

**Manned security services**
www.infologue.com
www.securebestvalue.org
www.securitywatchdog.co.uk

**National Neighbourhood Watch Association**
www.nwatch.org.uk

**Professional Security magazine**
www.professionalsecurity.co.uk

**Office of the Information Commissioner**
*(responsible for Freedom of Information and Data Protection legislation; formerly the Data Protection Commissioner)*
www.dataprotection.gov.uk

**Security at Work**
www.securityatwork.org.uk

**Security by design**
www.securedbydesign.com

**Security information services**
www.hi-media.co.uk/uk_security
www.securityfocus.com
www.securitypark.co.uk

**Security Management magazine**
www.securitymanagement.com

*Refer also to* Professional Security magazine
*www.professionalsecurity.co.uk*
Security Management Today magazine
*www.smtdirect.co.uk*
UK Internet Security Directory
*www.hi-media.co.uk/uk_security*

# Annex C Checklists and schedules

# Appendix 1 Outline security strategy

The study findings highlighted the benefits of a strategic approach to managing security, based on an agreed policy (see the *National report*, and section 2.4 of this document). Below are aspects that institutions should consider including in such a policy.

## Key elements

a. Mission statement: agreed security policy and service aims that integrate with other strategic policies and plans such as the estates strategy, health and safety policies, risk strategy, and capital plans.

b. Key security objectives identified and costed for the next five years, thereafter updated as a five-year rolling plan.

c. Statements of security management and personal responsibilities for key staff and others. These should be closely aligned to statements in the institution's health and safety policy. Major, specific actions to be undertaken should be stated for each postholder.

d. Arrangements for implementing the security strategy.

e. Resources to be allocated. These should be identified and costed within the institution's operational budgets.

f. Staff training and advice for security staff and others, including induction training and continuing professional development.

g. Links with other support services and key posts within and outside the institution, to improve service delivery and co-ordination

h. Service level standards/agreements for in-house and contracted services. These should include service-related management statistics to support continuous improvement.

i. Systems to review the strategy and monitor its effectiveness, including annual reporting to underpin wider understanding of and support for personal safety, crime prevention and risk management initiatives.

## Annexes

The security policy could be supported by annexed documents covering the following:

a. Assessment of security threats and risks (as part of an overall risk management approach/procedures adopted by the institution).

b. Organisational security service arrangements.

c. In-house and contracted security arrangements.

d. Codes of practice for security staff (technical and operational manuals relating to assignment instructions/standing orders).

e. University financial regulations and procedures for the purchase of security equipment, etc.

f. Buildings protection – access controls, alarms, CCTV and so on.

g. Student residences – on campus and with private landlords.

h. Personal property – staff and students.

i. Multi-agency arrangements, such as local crime prevention organisations.

j. Access arrangements on campus for taxis, maintenance contractors, deliveries, and so on.

k. Implementation of specific security measures and initiatives, such as security and customer surveys, ID cards, alarms, lighting, and keys and locks.

l. Implementation of initiatives in response to issues such as: out of hours working; car park security; advice and liaison with students and staff regarding personal safety and crime awareness; security costs borne by academic and administrative departments as part of devolved budgets.

## Appendix 2 Roles and responsibilities for security staff

The following is a generic listing of roles and responsibilities for the institution's security team, based on the requirement for an appropriate blend of technical expertise, practical knowledge and general management skills. Team members will include managers, supervisors, security officers and administrative staff, as well as other support staff dealing with, for example, caretaking, portering and car parking.

The institution can assess its present arrangements by comparing them with the following checklist. The checklist can be modified to meet the requirements of the institution, including any additional items, which should be identified by the head of security. The need for team members to liaise with other support services staff will vary, depending on their specific roles and responsibilities, for example, pastoral care of students.

| Responsibilities/duties | Key task: Yes/No? | Part of existing duties of security team: Yes/No? If yes, who? | Actions |
|---|---|---|---|
| **Security environment** | | | |
| All aspects of security arrangements for single and multi-project building programmes, involving security by design for all capital building and maintenance work – in particular:<br>• Initial consultation<br>• Liaison<br>• Implementation<br>• Pre and post-occupancy reviews.<br>Implementation of security systems for all buildings and installed services.<br>Introduction of an integrated control room for campus security. | | | |
| **Legislation, quality and standards** | | | |
| Ensuring compliance with legislation relating to security contracts, working conditions and employment.<br>Introducing and maintaining effective 'good housekeeping' and security operating procedures throughout the institution.<br>Introducing service level standards for security arrangements and procedures.<br>Introducing and updating operational procedural documents and statements of good practice regarding security services. | | | |

| Responsibilities/duties | Key task: Yes/No? | Part of existing duties of security team: Yes/No? If yes, who? | Actions |
|---|---|---|---|
| Undertaking audit and validation functions of security services for quality and standards, and compliance with legislation, statutory regulations and procedures. | | | |
| **Insurance, assessment and management of security risks** | | | |
| Organising comprehensive and selective risk assessment surveys of campus buildings, as required.<br>Analysing risks survey data, disseminating timely management information, and updating security plans and programmes. | | | |
| **Security strategy** | | | |
| Overseeing the formulation and implementation of a funded strategic policy for security.<br>Ensuring that the security strategy integrates with the aims and objectives of other strategic documents covering core business activities, space management and the environment.<br>Instigation of core service policies for security services – which are underpinned by security staff training and development. For example, these could relate to the implementation of a multi-agency approach by the institution for its security services; the integration of pastoral care arrangements for students and the role to be undertaken by security staff; and so on. | | | |
| **Security management structures and links with other services** | | | |
| Implementing security staff rota systems for all buildings and installed services.<br>Implementing systems for reporting incidents.<br>Internal and external liaison arrangements for security services | | | |
| **Raising awareness of crime, and crime prevention** | | | |
| Promoting personal safety and crime prevention advice to staff and students. | | | |

| Responsibilities/duties | Key task: Yes/No? | Part of existing duties of security team: Yes/No? If yes, who? | Actions |
|---|---|---|---|
| **Procurement** | | | |
| Managing supply contracts for security services and related processes/systems.<br>Undertaking periodic contract management and procurement reviews of security services.<br>Introducing and maintaining review procedures to demonstrate to the institution's senior management and other relevant staff, that the security service gives value for money. | | | |
| **Staff training and development** | | | |
| Identifying the institution's training needs for security-related staff skills and understanding.<br>Identifying and introducing a training policy and programmes for security staff.<br>Developing interpersonal, communications, people-management and risk evaluation skills for staff. | | | |
| **Balancing technology with other security measures and resources** | | | |
| Maintaining comprehensive and up-to-date security registers, surveys and record systems.<br>Using financial, planning, and management systems; including the prioritisation of responses to security incidents. | | | |
| **Funding and service performance** | | | |
| Identifying and reporting to members of the governing committee and senior management team, management statistics for security services covering standards, investment, planning and staff.<br>Identifying suitable opportunities for cost-effective security projects, in new or existing premises. | | | |
| Use of diagnostic and problem-solving systems and techniques for managing responses to security incidents.  This includes establishing investment appraisal criteria and documentation, and assessing risks to core business activities. | | | |

| Responsibilities/duties | Key task: Yes/No? | Part of existing duties of security team: Yes/No? If yes, who? | Actions |
|---|---|---|---|
| Formulating an investment programme for funding cost-effective security projects, to satisfy the short, medium and long-term objectives of the institution.<br>Providing timely management information about the performance and cost-benefits of security services. | | | |

**Summary**

| Post-holder(s) | Review findings (Comparison of team post-holders responsibilities and duties with key tasks) | Actions |
|---|---|---|
| Security managers | | |
| Security supervisors | | |
| Security officers | | |
| Administrative staff | | |
| Maintenance, caretaking, cleaning, portering, mail delivery, car parking and other support /ancillary staff | | |

# Appendix 3 Security equipment: repair or replace?

Decisions to implement and update security equipment should be consistent with the objectives identified in the institution’s security policy and strategy.

This checklist is designed to help institutions decide whether to repair or replace installed security equipment and components. The checklist can be modified to meet the requirements of the institution; any additional items should be identified by the head of security. The outcomes, and an assessment of the risks and priorities for the institution if the component fails, will inform the final decision that is consistent with its security objectives.

| **Considerations** | **Options** | **Tick only one box per section** | |
|---|---|---|---|
| | | **Repair** | **Replace** |
| **Age: consider the age of the equipment in relation to its expected economic life** | | | |
| Age is less than expected economic life (eg, 2-5 years)/(5-10 years) | Consider repair, if condition is very satisfactory. | | |
| Age is at or close to expected economic life (eg, +/- 18 months) | Consider repair and/or partial replacement, if condition is satisfactory in part. | | |
| Age is more than expected economic life (eg, 2-5 years)/(5-10 years) | Consider replacement, if condition is very unsatisfactory. | | |
| **Condition: assess the current condition of the equipment, and any underlying trend in condition, in relation to its operating performance** | | | |
| Current overall condition, and the underlying condition trend, is very satisfactory and consistent | Continue to repair as necessary. Priority is low. | | |
| Current condition, and the underlying condition trend, is satisfactory in part and therefore subject to qualification (which should be stated, either in regard to the equipment’s condition and/or its rate of deterioration) | Consider repair and/or partial replacement. Priority is medium to high. Repair as required, but consider replacing worst parts and, if appropriate, start to plan for replacing all or part. If the rate of deterioration is high, then appraise condition more frequently. If repair is not cost-effective, then replace. | | |
| Current overall condition, and the underlying condition trend, is very unsatisfactory (giving cause for concern that the trend in the rate of deterioration is rapid and/or hazardous and/or liable to contravene legislation) | Replace as a high priority. | | |

| Considerations | Options | Tick only one box per section | |
|---|---|---|---|
| | | Repair | Replace |
| **Maintenance costs: assess maintenance costs as a proportion of the capital cost, and whether replacement provides clear cost-benefits over the life-cycle of the equipment.** | | | |
| Maintenance costs are low | Continue to repair. | | |
| Maintenance costs are average | Consider repair and/or partial replacement. Repair as required, but consider replacing worst parts and, if appropriate, start to plan for replacing all or part. If the rate of deterioration is rapid, then appraise condition more frequently. If repair is not cost-effective, then replace. | | |
| Maintenance costs are high | Replace, if life-cycle costing indicates positive cost-benefits. | | |
| **Energy cost-benefits: Identify the current energy costs of the equipment as a proportion of its operating costs, and whether energy cost-savings indicate that overall replacement is cost-effective.** | | | |
| Energy cost-benefits are high | Replace, if positive cost-benefits indicated. | | |
| Energy cost-benefits are average | Consider repair and/or partial replacement, as appropriate. | | |
| Energy cost-benefits are low | Continue to repair. | | |
| **Technology and design opportunities: evaluate the continued 'fitness for purpose' of the equipment and whether developments in technology and design indicate that overall replacement provides clear cost-benefits.** | | | |
| Fitness for purpose is very satisfactory | Continue to repair. | | |
| Fitness for purpose is satisfactory | Consider repair and/or partial replacement, as appropriate. | | |
| Fitness for purpose is unsatisfactory | Replace. | | |
| **Spare parts : confirm that spare parts for the equipment are readily available at a reasonable cost.** | | | |
| Spare parts are readily available at a reasonable cost | Consider repair, if other factors indicate cost-benefits. | | |
| Spare parts are not readily available at a reasonable cost | Replace, even if other factors indicate otherwise. Circumstances would indicate that advances in technology, etc, have taken place. | | |

**Other comments:**

**Summary**

| Considerations | Repair | Replace | Comments |
|---|---|---|---|
| **Age** | | | |
| **Condition** | | | |
| **Maintenance costs** | | | |
| **Energy costs** | | | |
| **Technology and design** | | | |
| **Spare parts** | | | |
| | | | |
| **Risk to institution if equipment fails (on a scale of 1-5 where 5 is greatest):** | | | |
| **Priority (on a scale of 1-9 where 9 is greatest):** | | | |
| **Security policy and strategy objective:** | | | |
| **Final decision and actions:** | | | |
| | | | |

## Appendix 4 Legislation and good practice guidance

| *Legislation and statutory regulations* |
|---|
| Access to Neighbouring Land Act 1992 |
| Animals Act 1971 |
| Building Act 1984 |
| Building Regulations 1985 and 1991, as amended in 1999 |
| Caravan Sites Act 1965 |
| Civic Government (Scotland) Act 1982 |
| Companies Acts 1985 to 1989 |
| Computer Misuse Act 1990 |
| Consumer Protection Act 1987 |
| Control of Pollution Act 1974 (Scotland) |
| Control of Substances Hazardous to Health Regulations 1999 |
| Crime and Disorder Act 1998 |
| Criminal Damage Act 1971 |
| Criminal Justice Act 1988 |
| Criminal Justice and Police Act 2001 |
| Criminal Justice and Public Order Act 1994 |
| Criminal Justice (Scotland) Act 1980 |
| Criminal Law Acts 1967 and 1977 |
| Criminal Procedure (Scotland) Act 1995 |
| Dangerous Dogs Act 1991 |
| Data Protection Act 1998 |
| Disability Discrimination Act 1995 |
| Electricity at Work Regulations 1989 |
| Electronic Communications Act 2000 |
| Employers' Liability (Compulsory Insurance) Act 1969 |
| Environmental Protection Act 1990 |
| Factories Act 1961 |
| Firearms Act 1968 |
| Firearms (Amendment) Act 1994 |
| Fire Certificates (Special Premises) Regulations 1976 |
| Fire Precautions Act 1971 (and as amended) |
| Fire Precautions (Workplace) Regulations 1997 |
| Fire Safety Act 2000 |
| Fire Safety and Places of Sport Act 1987 |

| *Legislation and statutory regulations* |
|---|
| Food Safety Act 1990 |
| Forgery and Counterfeiting Act 1981 |
| Freedom of Information Act 2000 |
| Guard Dogs Act 1975 |
| Health & Safety (Safety Signs and Signals) Regulations 1996 |
| Health and Safety at Work etc Act 1974 |
| Highly Flammable Liquids and Liquefied Petroleum Gases Regulations 1972 |
| Highways Act 1980 |
| Housing Act 1985 |
| Human Rights Act 1998 |
| Interception of Communications Act 1985 |
| Knives Act 1997 |
| Licensing Act 1964 |
| London Local Authorities Act 1991 |
| Management of Health and Safety at Work Regulations 1992 and 1999 |
| Manual Handling Operations Regulations 1992 |
| Misuse of Drugs Act 1971 |
| Noise and Statutory Nuisance Act 1993 |
| Noise at Work Regulations 1989 |
| Occupiers' Liability (Scotland) Act 1960 |
| Occupiers' Liability Acts 1957 and 1984 |
| Offences Against the Person Act 1961 |
| Offensive Weapons Act 1996 |
| Offices, Shops and Railway Premises Act 1963 |
| Offices, Shops and Railways Premises (Hoists and Lifts) Regulations 1968 |
| Petroleum Consolidation Act 1928 |
| Police Acts 1964 and 1997 |
| Police and Criminal Evidence Act (PACE) 1984 |
| Police Order Act 1996 |
| Prevention of Crime Act 1953 |
| Private Security Industry Act 2001 |
| Protection from Harassment Act 1997 |
| Public Order Act 1986 |
| Regulation of Investigatory Powers Act 2000 |
| Rehabilitation of Offenders Act 1974 |

| *Legislation and statutory regulations* |
|---|
| Reporting of Injuries, Diseases and Dangerous Occurrences (RIDDOR) Regulations (as revised) 1995 |
| Sexual Offences Act 1956 |
| Street Offences Act 1959 |
| Telecommunications (Fraud) Act 1997 |
| Theft Acts of 1968 and 1978 |
| Theft (Amendment) Act 1996 |
| Town and Country Planning Act 1990 |
| Town and Country Planning General Development Order 1988 |
| Trade Descriptions Acts of 1968 and 1978 |
| Transfer of Undertakings (Protection of Employment) Regulations 1981 |
| Trespass (Scotland) Act 1965 |
| Unfair Contract Terms Act 1977 |
| Vagrancy Act 1824 |
| Wireless Telegraphy Act 1949 |
| Working Time Directive (EU 93/104/EC) |
| Working Time Regulations 1998 |
| Workplace (Health, Safety and Welfare) Regulations 1992 |

| *Codes of practice and good practice guidelines* |
|---|
| BS 476: Fire tests on building materials and structures |
| BS 1722 (1999): Fences |
| BS 3621 (1980): Specification for thief-resistant locks |
| BS 4102 (1976): Steel wire for fences |
| BS 4737: Intruder alarm systems |
| BS 5051: Bullet resistant glazing for interior and exterior use |
| BS 5266:Emergency lighting – maintenance and records |
| BS 5306 (1990): Fire extinguishing installations and equipment on premises - specification for sprinkler systems |
| BS 5357: Code of practice for the installation of security glazing |
| BS 5445: Components of fire detection systems |
| BS 5544: Specification for anti-bandit glazing (glazing resistant to manual attack) |
| BS 5839: Fire detection and alarm systems for buildings |
| BS 5979 (1993): Code of practice for remote centres for intruder alarm systems |
| BS 6180: Code of practice for protective barriers in and about buildings |
| BS 6206 (1981): Specification for impact performance requirements for flat safety glass and safety plastics for use in buildings |

| *Codes of practice and good practice guidelines* |
|---|
| BS 6262 (1994): Code of practice for glazing in buildings |
| BS 6266: Fire protection systems for electronic data processing installations |
| BS 7499 (1998): Manned security services: code of practice for static guarding, mobile patrol and key-holding services |
| BS 7799: Code of practice for information security management |
| Risk assessment and risk management - Guide to BS 7799 (BSI) |
| BS 7858 (1996): Security screening of personnel employed in a security environment |
| BS 7872 (1996): Code of practice for the operation of cash-in-transit (Collection and Delivery) |
| BS 7931 (1998): Code of practice for secure carriage of parcels |
| BS 7958 (1999): Code of practice for the management and operation of closed circuit television monitoring |
| BS 7960 (1999): Code of practice for door supervisors/stewards |
| BS 8220: Security of buildings against crime |
| BS EN ISO 9002 (1994): Quality systems (formerly BS 5750) |
| BS EN ISO 50130 (1 to 5): Alarm systems, alarm systems terminology, symbols, EMC immunity |
| BS EN ISO 50131 (1 to 7): Intruder alarms |
| BS EN ISO 50132: CCTV systems |
| BS EN ISO 50133 (1 to 7): Access control systems – system requirements, general requirements – components, processing, display and programme equipment, access point actuator, power supply and application guidelines |
| BS EN ISO 50136: Signalling systems |
| BS EN ISO 60081 (1994): Specification for intruder fluorescent lamps for general lighting service |
| CCTV – looking out for you (Home Office) |
| Code of practice for CCTV surveillance – Data Protection Act 1998 |
| Code of practice for the construction of buildings (published by the Loss Prevention Council) |
| Glazing materials and protection (Approved Document N 1992, Building Regulations 1991) |
| Information for Employers about the Fire Precautions (Workplace) Regulations 1997 (Home Office publication) |
| Loss Prevention Certification Board (LPS 1242): requirements and test methods for classifying cylinders for locks (BS EN ISO 1303 1998) |
| NACP1: Security screening for personnel (see also BS7858) |
| NACP2: Customer communications |
| NACP3: Management of sub-contracting |
| NACP4: Compilation of (quality) control manual |
| NACP5: Management of customer complaints |
| NACP10: Management of false (intruder) alarms |
| NACP11: Planning, installation and maintenance of intruder alarms |
| NACP12: Wire-free inter-connections within intruder alarms |

| *Codes of practice and good practice guidelines* |
|---|
| NACP13: Intruder alarms for high security premises (see also BS7042) |
| NACP20: Code of practice for planning, installation and maintenance of closed circuit television systems |
| NACP30: Code of Practice for planning, installation and maintenance of access control systems |
| Planning Out Crime (Department of the Environment - Circular 5/94) |
| Physical protection devices for personal computers and similar devices (Loss Prevention Council - LPS 1214, January 1995) |
| Rules for automatic sprinkler installations (Loss Prevention Council, 1999) |
| Security in the Community - (NACOSS, 181/2000) |
| Security, overall safety and durability of walls (BRE, Good Buildings Guide - 14) |
| Scheme for the application of European standards for intruder alarms: (BSI Published Document 6662, 2000) |
| Wheel clamping on private land (Home Office, 1993) |

# Appendix 5 Service level statements and agreements

**Service level statement (SLS)**

Enables the service provider to inform customers (end-users) of the standards of service they can expect, and what remedies will be offered in the event of failure to meet the set standards. It exists in addition to a formal contract, or service level agreement. The service provider is usually expected to draft and sign the statement. It is based on the description of the work, performance targets and quality standards in the contract for bought-in services.

**Service level agreement (SLA)**

The SLA is what the institution requires from the service provider. It is a formal document that defines a working relationship between different parts of the institution. Because an HEI is a single legal entity (excluding its captive 'subsidiary' companies), there cannot be contracts between different parts of that entity. The SLA may take the place of a contract. It would typically be used where there is internal charging for the provision of an in-house service, or where the service is so critical to the customer (end-user) that a formal written agreement is required.

Further guidance concerning service level statements and service level agreements may be obtained from:
*Guidance on the procurement of services* (Joint Procurement Policy and Strategy Group, Volumes 1 and 2, September 2000)

*Facilities management – improving the management of support services in higher education* (National Report, HEFCE 00/14).

**List of abbreviations**

| | |
|---|---|
| AUCSO | Association of University Chief Security Officers |
| BSIA | British Security Industry Association |
| CCTV | Closed circuit television |
| CIBSE | Chartered Institution of Building Services Engineers |
| CPE | Continuous professional education |
| FE | Further education |
| FEC | Further education college |
| HE | Higher education |
| HEFCE | Higher Education Funding Council for England |
| HEI | Higher education institution |
| ID | Identity |
| IT | Information technology |
| JPPSG | Joint Procurement Policy and Strategy Group |
| NACOSS | National Approval Council for Security Systems |
| SITO | Security Industry Training Organisation |
| SLA | Service level agreement |
| SLS | Service level standards |
| SMT | Senior management team |
| TUPE | Transfer of Undertakings (Protection of Employment) Regulations |