

ELECTRONIC SECURITY SYSTEMS POLICY

1.0 Purpose

The purpose of this policy is to provide a framework for the authorisation and control of electronic security systems for the University of Queensland.

The University has in place a comprehensive and integrated security system covering all major and some minor sites. The system is comprised of “Siemens” access control equipment and monitoring software, a dedicated PABX intercom system and an integrated closed circuit television system. All these systems communicate with a 24 hour central security monitoring station on the St Lucia campus. In summary:

- 1.1 Electronic Security Systems (ESS) are used throughout the University to increase the general security and access of Buildings and other places that have a requirement for increased security measures.
 - 1.2 Access Control Systems should be used as a tool to control, monitor and restrict the flow of persons to certain areas or buildings.
 - 1.3 Security Monitoring Systems provide a high level of security for a designated area which, when activated, will elicit an immediate physical response from the Security Section.
 - 1.4 Closed Circuit Television systems (CCTV) are to be used as a tool to monitor all security aspects of the University campuses, in conjunction with other security systems
 - 1.5 Security telephony system is used for direct communications with the Security Section, generally in emergency situations.
 - 1.6 All Electronic Security Systems installed on University sites are to be approved by the Manager Security (MS)

2.0 Scope

- 2.1 This policy applies to all Faculties, Schools, Departments Sections and all other areas on all University sites.
- 2.2 Assessments are carried out by Security Personnel, in the form of a Security Audit (refer PF267) and the results are provided in writing to the client.
- 2.3 Clients decide on what security measures they will adopt and advise the Manager Security accordingly.
- 2.4 Electronic Security Systems (ESS) include, but are not limited, to the following:
 - 2.4.1 Access control systems(currently Siemens is the approved system for the use on University sites)
 - 2.4.2 Security alarm systems(currently Concept systems are the approved system on University sites)
 - 2.4.3 Security telephony system (currently Wayphone, Emphone and NEC are the approved systems on University sites)
 - 2.4.4 Closed Circuit Television Systems (CCTV). A wide range of equipment and systems is used for the University CCTV network, however, there are three categories of CCTV systems:
 - 2.4.4.1 Primary external units exclusively for Security use for observations on external areas of campus.
 - 2.4.4.2 Secondary internal building units for Security use for observations of building areas on campus.
 - 2.4.2.3 A local DVR system for Departmental and Security use for observations and security of Faculties, Schools, Departments and other areas within buildings
 - 2.4.4.4 Covert CCTV systems used only by the Security Section in accordance with the “Use of Covert Camera Systems Policy PF-S/v3-op19”
- 2.5 Electronic security Systems are developed, authorised and administered by the Security section under the guidance of MS and the Technical Officer Security (TOS)



3.0 References

- 3.1 Security Audit Brief (PF267)
- 3.2 Australian Design Standards
- 3.3 University Design Standards

4.0 Responsibilities

4.1 Systems Administration & Monitoring Responsibilities

- 4.1.1 University Departments occupying a building are responsible for the day-to-day requirements of their internal access control systems unless transfer of responsibility to the Security Section is arranged through mutual agreement.
- 4.1.2 The Security Section will be responsible for:
 - remotely monitoring the system functions
 - issue cards in conjunction with user requirements. University Faculties, Schools, and other areas are encouraged to manage the issue and data processing of cards through a Siemens site licence that is approved by Security and funded by the Faculty, School or other areas.
 - operate, administer and maintain perimeter entrance access controls for all University Buildings.

4.2 Funding

- 4.2.1 All University and private tenants or users of University buildings are responsible for the funding of any access or security systems and all associated costs with the exception of internal areas which MS determines to require a higher level of access control than that provided by keys and locks. In such cases electronic access control requirements will be funded by sources other than the functional organisation.
- 4.2.2 On new construction and rehabilitation projects the cost of installation of any access or security system is to be charged against the project.
- 4.2.3 The University of Queensland will be responsible for maintenance and repair cost of access control and security systems when installed for University convenience, up to and including the external extremities of a building.
- 4.2.4 Faculties, Schools and other areas are responsible for the cost of installation, maintenance and repairs to electronic security systems installed in their areas.
- 4.2.5 Private tenants and the Student Union are responsible for the cost of maintenance and repairs to access control and security systems installed on their premises.
- 4.2.6 When an installed Electronic Security or Access Control System has reached the obsolescent stage and it is not a viable proposition to repair, the replacement of the system is the responsibility of the user ie: Department, Faculty etc.

4.3 University Buildings

Operation of entry Access Control Systems in buildings constructed by the University and having shared leased occupancy will be fully administered by the Security Section and controlled from the Central Security Monitoring Station (CSMS). This arrangement is necessary in order to minimise the equipment needed to control access to individual occupancy areas and to preclude access to and possible corruption of a common building database by unauthorised persons. Faculties, Schools and Departments are responsible for the cost of maintaining and end life-cycle replacement cost for the electronic security systems in their area of control.

- 4.3.1 The Buildings Occupants are responsible for:
- 4.3.1.1 Staff Cards - obtaining identification photographs through the UniCard Desk, details of which are then passed to security for processing.
Student Cards – Departments obtaining a supply of encoded access cards from Security and issuing to students; supplying cardholders details to security for processing on the access system and validating the card for use;
NOTE: University Faculties, Schools and other areas are encouraged to manage the issue and data processing of access cards through a Siemens site licence that is approved by security and funded by the Faculty, School of other areas.
 - 4.3.1.2 Determining the areas of access within the building for each cardholder.
 - 4.3.1.3 Determining the times of access for each cardholder.
 - 4.3.1.4 Reimbursing Security Section for all the costs of blank magnetic card production via an Inter-Departmental Requisition Form, (point 6.0 for schedule fees).
 - 4.3.1.5 Retrieving any access control cards from departing personnel.
 - 4.3.1.6 Conducting regular audits of card issue and returns.
- 4.3.2 The Security Section is responsible for:
- 4.3.2.1 Allocating a number for each access card.
 - 4.3.2.2 Entering the card holder's particulars, access levels, code, etc in the employee database unless other arrangements exist.
 - 4.3.2.3 Deleting access control numbers held by departing personnel when managing the database.
 - 4.3.2.4 Maintaining a register of all card holders on the access database.
- 4.4 Security Audits
Full consultation between tenants and the Security Section is required to determine user requirements via the [Security Audit Process – PF-S/v3-op9](#).

5.0 Action

- 5.1 Installation
The University of Queensland adopts Australian Design Standards numbers: AS 2201 and AS 3000, which cover the installation and use of Electronic Access Control and Security Monitoring Systems along with University Guidelines for project construction. All Access Control and Security Systems must be installed in accordance with these design standards. Any future additions or alterations must conform with these design standards, be compatible with the University Network, be installed with the approval of and under supervision of MS and organised by MS through the relevant contractors and monitored by the University Security Section.
- 5.2 The Network is located in the Central Security Control Room and is monitored on a 24-hour basis.
- 5.3 Commissioning
Prior to any new installation or alterations to existing access control or security systems being accepted "on line", each system must be commissioned by the installer in the presence of the TOS and the Security Supervisor (SS). Only after all access and alarm points on the system have been successfully tested and proven, shall the system be accepted by the Security Section as being operational. Detailed installation drawings are to be provided by the commissioning installer to the TOS.
- 5.4 Bar Code & Magnetic and Smart Card Access Control System Procedures
- 5.4.1 System Description
The card access control network is supervised from the Central Security Monitoring Station (CSMS). This shall be linked by buss to individual access control modules in allocated

buildings, on or off the University Campus. The access control system is connected to the P&F network on the PFASCO domain.

5.4.2 Access Levels

The access level allocated to a user's card provides the conditions under which that card can be used ie. the time zone and doors. Access levels are created by the Security Section after discussions with the Department concerned.

5.4.3 Self-Contained Buildings

The Department controlling a building is responsible for providing the Security Section with all relevant details relating to access card users. This includes:

- 5.4.3.1 Determining the areas of access within the building for each cardholder.
- 5.4.3.2 Determining the times of access for each cardholder.
- 5.4.3.3 Maintaining a register of cardholders.
- 5.4.3.4 Supplying the Security Section with a detailed access list.
- 5.4.3.5 Meeting all the costs of card production by the Security Section via an Inter-Departmental Requisition Form.
- 5.4.3.6 Conducting regular audits of card issues and returns.

6.0 Fee Schedule

This section sets the fees for issue of all access cards for use within all sites of The University of Queensland.

6.1 Management Fee For All Holders (including student card holders)

Existing cardholders including barcode, magnetic and student cards:

Fee for changes, upgrading and encoding etc.= \$2.00 per card, per management year.

Faculties, Schools and Departments who manage their own student access cards are exempt from this fee.

6.2 Cost of Barcode Security Cards (for Gehrman Building only)

Hard plastic barcode cards supplied by Security:= \$4.50 per card

6.3 Cost of Hard Plastic Magnetic Cards

Hard plastic magnetic access cards supplied by Security: = \$3.50 per card

6.4 Payment Details

6.4.1 Management Fee (All Access Users)

Accounts for all access users will be issued in the month of September of any one financial year. Accounts will be for the current year and include all processing of all cards for each Faculty, Department or School.

Payment is to be processed through the Interdepartmental Requisition (Store Catalogue No. 12076 available from the University Stores (including student cards).

6.4.2 Records

Records of all cards processed by the Security Section will be maintained by the TOS and any queries in relation to access cards can be directed to the TOS by fax: 3365 1600.

7.0 Video Recordings

The Security Section maintains a system of CCTV cameras at various locations at St Lucia and Ipswich Campuses. These cameras are recorded on video and hard disk. Other departments and organisations within the University also maintain their own CCTV cameras and recording equipment as part of their security systems. These are owned and maintained by individual departments and are separated from the Security Section's systems. At times various activities are recorded and the recordings may be required for identification and/or evidential purposes. This section sets out the policy to be followed in dealing with these matters.



7.1 Systems Under Control of the Security Section

- 7.1.1 During the course of routine enquiries and investigations the Security Supervisors may view recordings of CCTV cameras operated by the Section. Where the tape reveals evidence of offending, enquiries should be made to identify the offender/s and the tape retained as outlined in 7.1.4-6.
- 7.1.2 A request made by someone outside the Security Section for recordings of cameras operated by the Security Section to be viewed is to be made in writing to the Manager Security outlining the circumstances and reason for the request.
- 7.1.3 When approval is given the Manager will have a Security Supervisor view the tape.
- 7.1.4 If the recording provides evidence of offences being committed the Security Supervisor will place the tape in an envelope and record details on the envelope.
- 7.1.5 The tape is to be secured and retained pending the outcome of the investigation.
- 7.1.6 If the matter is reported to the Police the tape may be handed to the investigating Police Officer.
- 7.1.7 Where the recording is on hard disk a copy of the recording is to be made on compact disk and retained as per 7.1.3-5.

7.2 External Departmental CCTV

- 7.2.1 Occasionally a request may be made to the Security Section to view a recording of a camera owned by another department or organisation within the University. The person making the request is to be referred to the Manager of the department or organisation that owns the cameras.
- 7.2.2 Security Section members may at times attend complaints in which offending activity or other behaviour is recorded by a department or organisation that operates its own CCTV system.
- 7.2.3 Viewing the recording in these circumstances is the responsibility of the owner of the equipment.
- 7.2.4 If the equipment owner finds that the recording shows offending behaviour the investigating officer should view the tape with the owner with a view to identifying the offender.
- 7.2.5 If the incident involves criminal offending, the victim/complainant is to be advised to report the matter to the Police and advise the Police that the incident has been recorded.
- 7.2.6 The owner of the equipment is to be advised to secure the tape pending the Police investigation and make the recording available to the Police if required.
- 7.2.7 The investigating Security Officer should not take possession of the tape unless directed to do so by the Security Supervisor.