USQ SECURITY REVIEW

EXECUTIVE SUMMARY

USQ is undertaking a comprehensive and holistic review of its Security Services. The objective of the review is to develop a coordinated approach to the provision of security related services based upon existing and future need, utilising current and emerging technologies, innovations and industry best practice. Deliverables from this project will include the development of a Security Policy.

The review will assess the current and future provision and management of the following:-

- Electronic access control
- Closed Circuit Television & monitoring
- Duress / panic buttons
- Policing of access control
- CPTED (crime prevention through environmental design)
- Security service synergies with other Facilities Management functions
- Crime opportunity reduction
- Security services profile, awareness & education
- Special events coverage
- Strategic relationships with Local Council and Police
- Contract Security service scope review and alignment
- USQ Club security
- Notification system for security and energy breaches
- Key management
- Security software systems
- Security office

Review existing and provide recommendations

- Standing instructions for security guards
- Guard patrol methods and transportation
- Guard reporting methods/tools
- Security Services involvement with BCP (business continuity planning) and campus Emergencies
- USQ Security staff levels and role
- Frequency and nature of insecurity incidents
- Campus lighting
- Alarm systems and monitoring (including fire alarms)
- Location of fire monitoring equipment
- Staff I.D and smart card integration

Desired Outcomes

Best practice Security management, technique and policy. New technology/techniques explored and integrated or flagged for future integration where practical. CCTV position planning,

management and master plan for future expansion. Access control master plan developed. CPTED master plan developed. Policy recommendations provided.

Note: This security review will not encompass any I.T. related security, unless it specifically relates to the integrity of CCTV, access control or fire, intruder, duress or temperature alarm systems.

Stage 1 – Security Management Systems Review and Policy Development

Conduct a comprehensive review and gap analysis of current security systems. Provide a threat assessment with the primary objective of establishing priorities for "Stage 2 – Security Technology Master Plan". Coordinate "consultation and information gathering sessions" with key USQ stakeholders. Develop guidelines and policy for the management of USQ Security, access control and CCTV. All policies must be consistent with the new policy framework recently introduced at USQ.

Key deliverables

I. Executive outline of existing Security systems, processes and documentation.
II. Gap analysis of existing systems and processes compared with best practice.
    a. Encompass suitability, functionality, cost-effectiveness and operation of existing security measures.
III. Provide an assessment of priorities for the upgrade and/or deployment of CCTV and access control systems for Toowoomba, Fraser Coast and Springfield campuses and residential colleges.
IV. Recommendations for content of USQ Security Policy.
V. Recommendations for content of Access Control Policy.
VI. Recommendations for content of CCTV Policy.

Stage 2 – Security Technology Master Plan

Provide a comprehensive technology strategy and specification for the upgrade or provisioning of access control, CCTV and fire, intruder, duress and temperature alarm systems. Ensure that the proposal provides a sound platform for the future with an expandable architecture capable of accommodating new functions and emerging technologies. Investigate "green" technology. Ensure synergies with USQ "BMS" (Building Management System) are explored and reported on.

Key deliverables

I. Technology strategy (3-5 year plan) with rationalisation of recommended strategy/s and impact on existing infrastructure.
II. Assessment of the extent to which existing systems and peripheral devices can be retained.
III. Provide technical specifications and architecture for centrally controlled, managed and monitored CCTV, access control and alarm systems for all campuses and residential colleges.

IV. Determination of the type and nature of interfaces desired or required between new or existing electronic security systems and other USQ systems such as:-
    a. BMS
    b. Staff & student I.D card infrastructure
    c. Timetabling (Celcat)
    d. Human Resources
    e. Student enrolments
    f. Peoplesoft
V. Develop an Electronic Security Systems Technology Standard that addresses:-
    a. System resilience
    b. Redundancy arrangements
    c. Upgrade provisions
VI. Develop user training and familiarisation plan.
VII. Development of cost estimates for the staged implementation of the "Technology Master Plan".

Stage 3 – CPTED and Lighting

Review existing CPTED and campus lighting. Develop CPTED and lighting design and maintenance guidelines for the reference of:-

- Grounds maintenance.
- New building construction and refurbishment of existing facility projects.

Provide a comprehensive lighting assessment and positioning plan with particular emphasis on the proposed pedestrian thoroughfare upgrades (currently in a conceptual phase) to Toowoomba Campus. Review low voltage and solar lighting technology. Investigate synergies with USQ "BMS" (Building Management Systems).

Key deliverables

I. CPTED threat analysis.
II. CPTED design guidelines for referral by maintenance and new projects or refurbishments.
III. Lighting positioning plan and specification.
IV. Recommended staff training requirements