Security Management of Government Buildings

The Queensland Government has a responsibility to ensure its services are resilient to all foreseeable risks. In the context of security management, agencies need to implement processes and procedures to ensure the safety and security of people in government buildings and the continued delivery of government services.

Security management is the process of identifying, implementing and monitoring systems and processes for the protection of people and building assets against loss, misuse, damage or deprivation of use caused by deliberate acts. Building assets should have adequate security systems and processes in place to protect people, property, operational capability and information.

Efficient security management requires:

- assessing security risks (including the risks associated with terrorism) and their impacts on service delivery

- developing and implementing cost effective and appropriate measures to manage the risks

- monitoring the effectiveness of security measures and adjusting them as risks and circumstances change.

In this guideline, the term 'agencies' has the same meaning and is used interchangeably with 'departments' (as defined in s8 of the *Financial Accountability Act 2009*).

All agencies that control or administer buildings (regardless of whether they are tenants or owners) should comply with the requirements, processes and procedures for the security of Government buildings covered in the:

- *Government Asset Protection* (GAP) guides and toolbox

- *Guide for General Security Planning*

- *The Queensland Plan for the Protection of Government Assets from Terrorism*

- The *Australian/New Zealand Standard 31000:2009: Risk management – Principles and guidelines.*

For access to the whole-of-Government policy documents, agencies should contact the Queensland Police Service by email at Counter.Terrorism@police.qld.gov.au or by telephone on 07 3364 6791.

Benefits

Implementing efficient security management of government buildings:

- supports agency service delivery objectives

- minimises unnecessary losses or disruptions

- ensures Government meets its statutory obligations (e.g. duty of care) as the employer and building owner.

Risks

Inadequate or inappropriate security management can leave agencies exposed to unnecessary losses, damage, business disruption, injury to staff and/or litigation.

1.0   Security management process

A strategic approach to security management is essential for effective protection, prevention and emergency response. The following services related to the monitoring and operation of a security system (which are necessary to keep the building in a habitable and useable condition) should be considered:

- alarm monitoring

- mobile security patrols

- security audits

- provision of static security personnel

- other relevant protection measures in accordance with the principles and processes for on-site emergency response and business continuity in the *Queensland Plan for the Protection of Government Assets from Terrorism*.

The key stages of the security management process detailed below are consistent with the process of risk analysis and management outlined in the *Australian/New Zealand Standard 31000:2009: Risk management – Principles and guidelines.*

1.1   Establish the context

It is necessary to determine the assets and service delivery processes and procedures of the agency and the potential security incidents/threats which may impact upon them, for example:

- the key activities in the building with a particular focus on those which, if disrupted, could substantially affect the agency's ability to deliver its services

- the security threats to which the agency may be exposed

- where the vulnerabilities lie in relation to each of the threats regarded as plausible.

1.2   Identify, analyse and assess the risks

Agencies should consider what controls are in place, the likelihood of the situation taking place, whether there are any triggers which could signal the potential for such an event to happen, the consequences of such an occurrence and the cost to the organisation.

To complete the risk assessment, the level of the security risks should be evaluated and ranked according to their importance and the potential damage or harm that could result. Priorities should also be set to address each of these risks.

1.3   Identify and assess risk treatment options

In order to determine the most risk/cost effective security risk treatment options, agencies should identify options, assess options, prepare and implement treatment plans and analyse and evaluate residual risks.

Security measures can be broadly categorised as prevention, deterrence, detection or response, or a combination of these.

1.4   Develop a security management plan

A security management plan should be based on the recommended risk treatment options which:

- assign responsibilities for reporting, recording and analysing security incidents

- establish communication processes and (where applicable) ensure that relevant information is provided to key management committees

- institute a training and awareness program for key personnel and stakeholders

- include a process and timetable for the implementation of agreed physical and technical security procedures

- document performance criteria and ongoing monitoring processes for plan implementation

- determine funding requirements taking into consideration any existing service level agreement with the security provider and departmental plans for security/onsite emergency response and business continuity.

Building tenants should work cooperatively to develop collective arrangements for common areas of their building. Similarly, tenants of adjacent buildings need to implement mutually supportive security arrangements for their precinct.

In accordance with the requirements of the *Guide for General Security Planning,* a building security committee should be established in multi-tenanted buildings. The committee is responsible for periodically reviewing security risks and developing, implementing, reviewing and testing building security arrangements. The committee should comprise representatives from all tenants and from the building owner. A tenant representative with relevant authority should undertake the role of the chair of the committee.

In government buildings, where protective security services are coordinated by the Department of Housing and Public Works, the officer performing the function of the building service coordinator is responsible for implementing and testing security and emergency arrangements.

1.5   Monitor and review plans and feedback

The security management plan should be monitored to ensure its effectiveness. Improvements/changes in asset planning, maintenance procedures, risk management and security management plans could be triggered. by:

- responses to, or the impact of, security incidents on service delivery
- the results of testing exercises
- occurrence of security incidents not previously anticipated
- views of stakeholders regarding the effectiveness and value of security management and onsite emergency responses
- legislative changes
- performance of security operations.

The suite of guidelines which comprise the *Strategic Asset Management Framework* (available online at www.hpw.qld.gov.au) is organised under the following categories:

1. O**verview -** explains the principles and concepts of strategic asset management as they apply to buildings.

2. **Guidelines** - expand on key aspects of strategic asset management to inform decisions over the entire life-cycle of the asset.

3. **Decision-making methodologies and guidelines -** support agencies to implement best practice strategic management of buildings.

Enquiries should be directed to:

The Manager
Building Policy and Practice
Building Policy and Industry
Department of Housing and Public Works

GPO Box 2457
Brisbane Qld 4001

bip@hpw.qld.gov.au