SECURITY MANAGEMENT
Manage the application of security principles, practice, and procedure

level: 6
credit: 15
planned review date: March 2007
sub-field: Security

purpose: This unit standard is for people who work, or intend to work, as security managers or security consultants, and who need to manage the application of security principles, practice, and procedure.

People credited with this unit standard are able to:
- demonstrate knowledge of security principles, practice, and procedure;
- resolve security issues using security principles, practice, and procedure;
- provide information and advice on security issues.

entry information: Open.

accreditation option: Evaluation of documentation and visit by NZQA, industry and teaching professional in the same field from another provider.

moderation option: A centrally established and directed national moderation system has been set up by the ElectroTechnology Industry Training Organisation.

special notes: Legislation relevant to this unit standard includes:
- Building Act 1991;
- Children, Young Persons, and their Families Act 1989;
- Companies Act 1991;
- Crimes Act 1961;
- Employment Relations Act 2000;
- Evidence Act 1908;
- Fire Service Act 1975;
- Health and Safety in Employment Act 1992;
- New Zealand Bill of Rights Act 1990;
- Official Information Act 1992;
- Privacy Act 1993;
- Private Investigators and Security Guards Act 1974;
SECURITY MANAGEMENT
Manage the application of security principles, practice, and procedure

Protection of Personal and Property Rights Act 1980;
Resource Management Act 1991;
Secret Commissions Act 1910;
For assessment in countries other than New Zealand, the equivalent legislation in force in that country may be used.

2 Definitions
Analysis - the systematic examination and organisation of information.
Assets - in terms of security, assets are people and their activities, physical and intellectual property, information, and functions, processes and systems.
Best practice - an approved current method or way of doing something that, in the circumstances, achieves the required outcome.
Common security risks - risks common to most sites including but not limited to: trespass and unauthorised access; unsafe, disorderly, or disruptive behaviour; deliberate damage and destruction; other crime including theft, burglary, robbery and assault; safety and security breaches and incidents; emergencies or critical incidents resulting from fire, structural damage or failure, accidents, critical medical conditions, natural disasters including storms and earthquakes, flooding, leaks and spills of hazardous substances, and process and system failures, loss or compromise of information.
Duty of care - the legal and professional responsibility of a person or organisation to take due and proper care in their work.
Evaluation - the examination and comparison of information against accepted or required standards and/or other criteria to determine its value and relevance.
Physical risk - risk from physical threats to people, activities, and assets including crime, other inimical activities, natural events, and fire.
Policy - a plan of action adopted or pursued by an organisation.
Procedure - a way of acting or progressing, especially an established method.
SECURITY MANAGEMENT
Manage the application of security principles, practice, and procedure

Protective security - the systematic application of resources, systems and other measures to protect people, property, information and other assets, and activities, from physical risk.
Risk - the chance of something happening that will have an impact upon objectives, measured in terms of consequences and likelihood.
Sectors - include primary industry, manufacturing and processing, commercial services, financial, corporate, entertainment, hospitality, transport, communications, paramedical and medical, government, and domestic sectors of society and the economy.
Security - the protection of people, activities, and assets including information, from loss, damage, or harm.
Security consultant - a person providing independent professional security advice.
Security industry - persons, enterprises, organisations, and other entities that provide security and security-related products and services.
Security issues - issues relevant to security and security practitioners/managers and consultants including but not limited to common security risks, staff recruitment and employment; security events, incidents and breaches; complaints; information loss or compromise; employee theft or fraud; security policy, practice and procedure; misuse of drugs and or alcohol; misuse of property; staff and customer access; fire safety; security systems and equipment; personal safety.
Security manager - a person appointed to manage security in an organisation.
Security practice - strategies, actions and measures implemented to ensure security and accepted by industry as best practice.
Security principles - the general precepts on which security relies and which underpin best practice. Security principles include: cost - the cost of any security measures relates to or is proportional to assessed security risk and benefits; depth - provides multi-layer protection or sequential barriers; mutual Support - each security measure is supported and or protected by another; need to know - information about security matters is restricted to those who must know;
Elements and Performance Criteria

element 1
Demonstrate knowledge of security principles, practice, and procedure.

performance criteria

1.1 The purpose, scope, and objectives of security are described.
Range: two examples in each of three different sectors.

1.2 The principles on which protective security relies are explained.
Range: two examples in each of three different sectors.

1.3 Common security risks are described in terms of their nature, relevance, and impact.
Range: one example in each of three different sectors.

1.4 Security practice and procedure are described in terms of their nature, application, and effectiveness with reference to workplace examples.
Range: one example in each of three different sectors.

1.5 Security functions, resources, and structure are explained in terms of the products and services they provide with reference to workplace examples.
Range: one example in each of three different sectors.

element 2
Resolve security issues using security principles, practice, and procedure.

Range: issues - two common security risks and two other security issues from the definition of security issues.

**performance criteria**

2.1 Security issues are identified and assessed in terms of their nature, cause, and impact.

2.2 Immediate responses are consistent with relevant law and compliance guidelines including policy and procedure, and are prioritised in accordance with relevant factors.

Range: typical immediate responses - informing others, obtaining further information, damage control, liaison and co-operation, obtaining advice and support, obtaining technical or specialist support, ensuring safety.

2.3 Recommendations, strategies, and actions required to resolve identified security issues are stated and implemented in accordance with best practice, policy, and procedures.

**element 3**

Provide information and advice on security issues.

Range: issues - two common security risks and two other security issues from the definition of security issues;
issues relate to a specific entity or activity, or to a series of identified entities or activities.

**performance criteria**

3.1 Recipient's information and advice needs are met.

Range: needs - fit for purpose, scope, sufficiency, timeliness, structure and format, communication method, clarity, security, privacy.

3.2 Credibility of the information or advice is demonstrated by reference to the process used to produce it.
SECURITY MANAGEMENT
Manage the application of security principles, practice, and procedure


Comments on this unit standard

Please contact the ElectroTechnology Industry Training Organisation marilyn@etito.co.nz if you wish to suggest changes to the content of this unit standard.

Please Note
Providers must be accredited by the Qualifications Authority or a delegated inter-institutional body before they can register credits from assessment against unit standards or deliver courses of study leading to that assessment.

Industry Training Organisations must be accredited by the Qualifications Authority before they can register credits from assessment against unit standards.

Accredited providers and Industry Training Organisations assessing against unit standards must engage with the moderation system that applies to those standards.

Accreditation requirements and an outline of the moderation system that applies to this standard are outlined in the Accreditation and Moderation Action Plan (AMAP). The AMAP also includes useful information about special requirements for providers wishing to develop education and training programmes, such as minimum qualifications for tutors and assessors, and special resource requirements.

This unit standard is covered by AMAP 0003 which can be accessed at http://www.nzqa.govt.nz/framework/search/index.do.