



Australian Government

CPPSEC4022 Establish and implement ethics and governance arrangements for security businesses

Release: 1

CPPSEC4022 Establish and implement ethics and governance arrangements for security businesses

Modification History

Release 1 This version first released with CPP Property Services Training Package Release 9.0.

New unit.

Application

This unit specifies the skills and knowledge required to establish and implement ethical and governance arrangements to comply with legislative and regulatory responsibilities associated with managing a security business. It includes establishing, monitoring and communicating policies and procedures that ensure compliance with governance arrangements. It also includes understanding the ethical principles and security industry practices that guide professional conduct when performing security work, developing and implementing a code of conduct and taking necessary disciplinary actions for breaches of the code.

This unit is suitable for those using specialised knowledge to complete routine and non-routine tasks and using their own judgement to deal with predictable and sometimes unpredictable problems.

Legislative, regulatory or certification requirements apply in some states and territories to the provision of advice on security solutions, strategies, protocols and procedures. For further information, check with the relevant regulatory authority.

Pre-requisite Unit

None.

Unit Sector

Security/Risk management

Elements and Performance Criteria

Elements describe the essential outcomes.

Performance criteria describe what needs to be done to demonstrate achievement of the element.

1 Comply with governance requirements for security business.

1.1 Clarify governance requirements to comply with legislative and regulatory responsibilities associated with managing a security business in the jurisdiction of operation.

- | | | |
|---|---|---|
| | 1.2 | Establish or review required governance arrangements and associated policies and procedures in line with business plan. |
| | 1.3 | Confirm roles and responsibilities of all staff including accountabilities associated with business governance. |
| | 1.4 | Check to confirm required risk management processes, indemnities and insurances are in place and take corrective action where necessary to comply with legislative and regulatory responsibilities. |
| | 1.5 | Implement reporting systems to monitor business accountabilities and maintain records to comply with legislative and regulatory responsibilities. |
| | 1.6 | Communicate policies and procedures to relevant persons to ensure compliance with governance requirements. |
| 2 | Develop and implement code of conduct for ethical practice. | |
| | 2.1 | Source and review industry standards, codes and guidelines to understand the ethical principles that guide professional conduct in the security industry. |
| | 2.2 | Develop and document or review code of conduct linked to business mission, values and ethical principles. |
| | 2.3 | Describe and communicate to relevant persons ethical practice standards for privacy, confidentiality and information security associated with security work and equipment. |
| | 2.4 | Establish or review processes to handle complaints, monitor ethical practice and implement disciplinary actions for breaches of the code of conduct. |
| 3 | Monitor and review governance and ethical practices. | |
| | 3.1 | Schedule regular activities to monitor business and staff compliance against governance arrangements and code of conduct. |
| | 3.2 | Monitor ethical practice in the security industry and identify strategies to resolve discrepancies between business practice and security industry ethical standards. |
| | 3.3 | Audit internal governance arrangements and update |

policies and procedures as required to maintain currency and comply with legislative and regulatory requirements.

- 3.4 Monitor security work practices and complaints to resolve conflict, improve ethical practice and implement disciplinary actions for identified breaches of the code of conduct.

Foundation Skills

As well as the foundation skills explicit in the performance criteria of this unit, candidates require:

- oral communication skills to use negotiation to resolve conflict
- writing skills to prepare succinct and logically structured governance documentation.

Unit Mapping Information

No equivalent unit.

Links

Companion volumes to this training package are available at the VETNet website - <https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b>

Assessment Requirements for CPPSEC4022 Establish and implement ethics and governance arrangements for security businesses

Modification History

Release 1 This version first released with CPP Property Services Training Package Release 9.0.

New unit.

Performance Evidence

To demonstrate competency, a candidate must meet the performance criteria of this unit by establishing and implementing ethics and governance arrangements for a security business, involving:

- establish or review roles, responsibilities and governance accountabilities for:
 - one manager
 - two operational staff
 - one sub-contractor
- develop or review policies and procedures to ensure compliance with governance arrangements in the following areas:
 - indemnity, insurance and risk management
 - reporting and records maintenance
 - complaints and grievances
 - staff conduct, behaviour and disciplinary action
- develop or review a formal code of conduct that references current security industry standards, codes and guidelines, and through a review of security work practices and complaints, identify a minimum of two breaches of the code and suitable disciplinary actions for each breach.

Knowledge Evidence

To be competent in this unit, a candidate must demonstrate knowledge of:

- legislative and regulatory requirements associated with operating a security business in the jurisdiction of operation:
 - client service standards
 - key requirements of Corporations Act 2001 and actions by business owners and directors that may constitute a breach of duties
 - fair trading and consumer protection
 - licensing in the security industry

- privacy
- indicators of ethical practice in the security industry:
 - acting in the best interests of clients and workers
 - acting with honesty, fairness and professionalism
 - complying with fiduciary duties and obligations
 - demonstrating ethical practice when using surveillance equipment
 - engaging in fair and legal contracting practices and paying workers correct entitlements
 - maintaining client privacy and confidentiality and information security
 - maintaining independence and disclosing and managing potential conflicts of interest
 - maintaining and applying knowledge of legislative and regulatory responsibilities
 - using clear communication in all dealings with all parties to security business transactions including providing written and signed documents
- legal rights and obligations of different business ownership structures
- principles of ethical practice and their application in the security industry:
 - clear communication
 - client focus
 - client protection
 - confidentiality, privacy and information security
 - fairness
 - honesty
 - professional courtesy
 - respect
- purpose and application of Australian Security Industry Association Limited (ASIAL) standards, codes and guidelines:
 - cash-in-transit code of practice
 - code of ethics for the use and installation of closed circuit television (CCTV) equipment
 - codes and guidelines for best practice, including National Police Alarm Response Guideline, Electronic Home Security, AML/CTF compliance and the Care and Use of Security Dogs
- security industry standards, codes and guidelines that guide professional conduct
- types of behaviours considered unethical
- types of governance arrangements required to be implemented to ensure security businesses meet legislative and regulatory responsibilities
- workplace relations requirements associated with staff disciplinary actions.

Assessment Conditions

Assessors must meet the requirements for assessors contained in the Standards for Registered Training Organisations.

All individuals engaged by a licensed RTO for security licensing purposes must hold both a security trainers licence (where such a licence exists within the relevant jurisdiction) and the licence for performing the security activities for which the individual is providing training or assessment. Regulators may impose other assessor conditions to meet jurisdictional assessment requirements.

Assessment must be conducted in the workplace or in a simulated workplace environment. Candidates must have access to:

- security industry legislation, regulations, codes, standards and guidelines that apply to security business operation and governance in the jurisdiction of operation
- information technologies, resources and documentation required to achieve the performance evidence.

Links

Companion volumes to this training package are available at the VETNet website - <https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b>