Australian Government

Department of Education, Employment and Workplace Relations

PRSTS305A Identify and diagnose electronic security equipment/ system fault

Release: 1

PRSTS305A Identify and diagnose electronic security equipment/ system fault

Modification History

Not applicable.

Unit Descriptor

This competency standard covers the skills and knowledge required to identify and diagnose faults in electronic security equipment/systems. It requires the ability to ascertain normal operational functions and performance of a range of security equipment/systems, conduct fault-finding inspections and checks, systematically identify and diagnose faults, and accurately document and maintain information systems. This work applies in extra low voltage as defined through the Australian Standards As 2201 (1986) environments and would be carried out under routine supervision within organisational guidelines.
Functional Area: Core, Technical Security
This competency standard covers the skills and knowledge required to identify and diagnose faults in electronic security equipment/systems. It requires the ability to ascertain normal operational functions and performance of a range of security equipment/systems, conduct fault-finding inspections and checks, systematically identify and diagnose faults, and accurately document and maintain information systems. This work applies in extra low voltage as defined through the Australian Standards As 2201 (1986) environments and would be carried out under routine supervision within organisational guidelines.
Functional Area: Core, Technical Security

Application of the Unit

Not applicable.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

Not applicable.

Elements and Performance Criteria Pre-Content

Not applicable.

Elements and Performance Criteria

Elements and Performance Criteria

Element	Performance Criteria
1 Prepare for diagnosis of faults	1.1 Work order is reviewed and clarified with appropriate person(s) as required in accordance with organisational requirements
	1.2 Tools, equipment and materials are selected appropriate to job requirements and checked for operational effectiveness in accordance with manufacturer's specifications and organisational procedures
	1.3 Suitable personal protective equipment is selected, used and maintained in accordance with OHS and organisational requirements
	1.4 Potential and existing risks and hazards associated with security equipment / systems are identified and managed in accordance with OHS and organisational requirements
	1.5 Site access and specific site requirements are identified and appropriate arrangements made as required in accordance with client and organisational requirements
2 Diagnose faults	2.1 Safe operating practices are followed to remove risk of injury to self, others or security equipment / system in accordance with OHS and organisational requirements
	2.2 Reported faults are confirmed and normal operational functions and performance of security equipment / systems are ascertained in accordance with manufacturer's specifications
	2.3 Operational data and relevant information is accessed and appropriate inspections and tests are carried out in accordance with manufacturer's specifications and relevant industry standards

		2.4 Faults are systematically identified and diagnosed on the basis of an accurate assessment of inspection and test results, operational data and relevant information
		2.5 Personal limitations in identifying and diagnosing faults are promptly identified and assistance is sought from appropriate person(s) in accordance with organisational procedures
3	Complete and report diagnosis	3.1 Work is completed in an efficient and timely manner in accordance with work order and organisational requirements
		3.2 Notification of work completion is made to appropriate person(s) in accordance with organisational procedures
		3.3 Documentation is completed promptly and accurately and processed in accordance with client, legislative and organisational requirements
		3.4 Work area, tools and equipment are cleaned and stored in a secure and safe location in accordance with organisational requirements
		3.5 Waste from work activities is collected, treated and disposed of or recycled in accordance with organisational procedures and environmental policies

Required Skills and Knowledge

Not applicable.

Evidence Guide

The Evidence Guide identifies the requirements to be demonstrated to confirm competence for this unit. Assessment must confirm sufficient ability to use appropriate skills and knowledge to identify and diagnose electronic security equipment/system faults. Assessment of performance should be over a period of time covering all categories within the Range of Variables statements that are applicable in the learning environment.

What critical aspects are required for evidence of competency?

Clearly identify job requirements and organise appropriate tools, equipment and materials to carry out checks and testing of a range of security equipment and systems.

Confirm reported faults with client and ascertain normal performance of security equipment/system against manufacturer's specifications.

Follow safe and efficient work practices in the use of tools and equipment and effectively manage risks and hazards in the work area.

Conduct inspections and tests of security equipment/systems in a methodical manner and accurately identify and diagnose faults based on an assessment of test data, site variables, operational and historical information.

Clean and store tools and equipment, reinstate work area in a clear and safe condition, and update and submit all required documentation in an accurate and prompt manner.

What specific knowledge is needed to achieve the performance criteria?

Knowledge and understanding are essential to apply this standard in the workplace, to transfer the skills to other contexts and to deal with unplanned events. The knowledge requirements for this competency standard are listed below:

types, functions and specifications of security equipment/systems
operational principles of security equipment/systems
operational principles of data transmission networks
basics of circuit diagrams
electrical connections
electrical concepts (voltage, current, resistance and impedance)
common test equipment
tests to confirm equipment/system operation
fault finding techniques
common equipment/system faults
technical terms
common security equipment/system faults
building construction methods and types
cable identification and handling requirements
earthing systems arrangements and requirements
confined space procedures.

What specific skills are needed to achieve the performance criteria?

To achieve the performance criteria, some specific skills are required. These include the ability to:

read and interpret specifications, charts and diagrams
communicate in a clear and concise manner
demonstrate basic logic and lateral thinking processes
use appropriate tools and equipment
test security equipment/systems
read and interpret a multimeter

accurately identify and diagnose faults
identify and correctly handle cables
carry out soldering, welding, drilling and basic carpentry
work in confined spaces
methodically prioritise and organise work tasks
solve routine problems and trouble shoot
estimate resource requirements
apply safe and efficient work practices
prepare orders, invoices and supply requisitions.

What resources may be required for assessment?

Access to a suitable venue and equipment.
Access to plain English version of relevant statutes and procedures.
Assignment instructions, work plans and schedules, policy documents and duty statements.
Assessment instruments, including personal planner and assessment record book.
Access to a registered provider of assessment services.

What is required to achieve consistency of performance?

For valid and reliable assessment of this unit, the competency should be demonstrated over a period of time and observed by the assessor. The competency is to be demonstrated in a range of situations, which may include involvement in related activities normally experienced in the workplace.
Evidence of underpinning knowledge understanding of processes and principles can be gained through thorough questioning and by observation of previous work.

Assessment against this unit may involve the following:

Continuous assessment in a setting that simulates the conditions of performance described in the elements, performance criteria and range of variables statement that make up the unit.
Continuous assessment in the workplace, taking into account the range of variables affecting performance.
Self-assessment on the same terms as those described above.
Simulated assessment or critical incident assessment, provided that the critical incident involves assessment against performance criteria and an evaluation of underpinning knowledge and skill required to achieve the required performance outcomes.

Key competency levels

There are a number of processes that are learnt throughout work and life which are required in all jobs. They are fundamental processes and generally transferable to other work functions. Some of these are covered by the key competencies, although others may be added.
Information below highlights how these processes are applied in this competency standard.
1 - perform the process
2 - perform and administer the process
3 - perform, administer and design the process

How can **communication of ideas and information** be applied? (**2**)

Reported faults of security equipment/system may be verified in consultation with relevant persons.

How can **information be collected**, **analysed and organised**? (**2**)

Results of conducted inspections and tests may be accurately documented and organised in reports for analysis.

How are **activities planned and organised**? (**2**)

Fault-finding tests may be carried out systematically to ensure fault is effectively isolated and identified.

How can **team work** be applied? (**2**)
Personal limitations in identifying and diagnosing faults may be promptly identified and assistance sought from relevant persons.
How can the use of **mathematical ideas and techniques** be applied? (**2**)
Mathematical techniques may be used to accurately estimate resource requirements and prioritise work tasks.
How can **problem solving skills** be applied? (**2**)
Hazards and risks in the work area may be promptly identified and controlled to ensure safety of self, property and others.
How can the **use of technology** be applied? (**2**)
Technology may be used to communicate, source and record information. It may also be used to carry out testing activities.
The Evidence Guide identifies the requirements to be demonstrated to confirm competence for this unit. Assessment must confirm sufficient ability to use appropriate skills and knowledge to identify and diagnose electronic security equipment/system faults. Assessment of performance should be over a period of time covering all categories within the Range of Variables statements that are applicable in the learning environment.
What critical aspects are required for evidence of competency?
Clearly identify job requirements and organise appropriate tools, equipment and materials to carry out checks and testing of a range of security equipment and systems.
Confirm reported faults with client and ascertain normal performance of security equipment/system against manufacturer's specifications.
Follow safe and efficient work practices in the use of tools and equipment and effectively manage risks and hazards in the work area.
Conduct inspections and tests of security equipment/systems in a methodical manner and accurately identify and diagnose faults based on an assessment of test data, site variables, operational and historical information.
Clean and store tools and equipment, reinstate work area in a clear and safe condition, and update and submit all required documentation in an accurate and prompt manner.
What specific knowledge is needed to achieve the performance criteria?
Knowledge and understanding are essential to apply this standard in the workplace, to transfer the skills to other contexts and to deal with unplanned events. The knowledge requirements for this competency standard are listed below:
types, functions and specifications of security equipment/systems
operational principles of security equipment/systems
operational principles of data transmission networks
basics of circuit diagrams
electrical connections
electrical concepts (voltage, current, resistance and impedance)
common test equipment
tests to confirm equipment/system operation
fault finding techniques
common equipment/system faults
technical terms
common security equipment/system faults
building construction methods and types
cable identification and handling requirements
earthing systems arrangements and requirements

confined space procedures.

What specific skills are needed to achieve the performance criteria?

To achieve the performance criteria, some specific skills are required. These include the ability to:

read and interpret specifications, charts and diagrams
communicate in a clear and concise manner
demonstrate basic logic and lateral thinking processes
use appropriate tools and equipment
test security equipment/systems
read and interpret a multimeter
accurately identify and diagnose faults
identify and correctly handle cables
carry out soldering, welding, drilling and basic carpentry
work in confined spaces
methodically prioritise and organise work tasks
solve routine problems and trouble shoot
estimate resource requirements
apply safe and efficient work practices
prepare orders, invoices and supply requisitions.

What resources may be required for assessment?

Access to a suitable venue and equipment.
Access to plain English version of relevant statutes and procedures.
Assignment instructions, work plans and schedules, policy documents and duty statements.
Assessment instruments, including personal planner and assessment record book.
Access to a registered provider of assessment services.

What is required to achieve consistency of performance?

For valid and reliable assessment of this unit, the competency should be demonstrated over a period of time and observed by the assessor. The competency is to be demonstrated in a range of situations, which may include involvement in related activities normally experienced in the workplace.

Evidence of underpinning knowledge understanding of processes and principles can be gained through thorough questioning and by observation of previous work.

Assessment against this unit may involve the following:

Continuous assessment in a setting that simulates the conditions of performance described in the elements, performance criteria and range of variables statement that make up the unit.
Continuous assessment in the workplace, taking into account the range of variables affecting performance.
Self-assessment on the same terms as those described above.
Simulated assessment or critical incident assessment, provided that the critical incident involves assessment against performance criteria and an evaluation of underpinning knowledge and skill required to achieve the required performance outcomes.

Key competency levels

There are a number of processes that are learnt throughout work and life which are required in all jobs. They are fundamental processes and generally transferable to other work functions. Some of these are covered by the key competencies, although others may be added. Information below highlights how these processes are applied in this competency standard.

1 - perform the process
2 - perform and administer the process

3 - perform, administer and design the process
How can **communication of ideas and information** be applied? (**2**)
Reported faults of security equipment/system may be verified in consultation with relevant persons.
How can **information be collected**, **analysed and organised**? (**2**)
Results of conducted inspections and tests may be accurately documented and organised in reports for analysis.
How are **activities planned and organised**? (**2**)
Fault-finding tests may be carried out systematically to ensure fault is effectively isolated and identified.
How can **team work** be applied? (**2**)
Personal limitations in identifying and diagnosing faults may be promptly identified and assistance sought from relevant persons.
How can the use of **mathematical ideas and techniques** be applied? (**2**)
Mathematical techniques may be used to accurately estimate resource requirements and prioritise work tasks.
How can **problem solving skills** be applied? (**2**)
Hazards and risks in the work area may be promptly identified and controlled to ensure safety of self, property and others.
How can the **use of technology** be applied? (**2**)
Technology may be used to communicate, source and record information. It may also be used to carry out testing activities.

Range Statement

The Range of Variables provides information about the context in which the unit of competency is carried out. It allows for different work practices and work and knowledge requirements as well as for differences between organisations and workplaces. The following variables may be present for this particular unit:

Work order information may relate to:
work schedules
completion dates
job requirements and tasks
specific client requirements
access to site and specific site requirements
resource requirements
OHS requirements
compliance with relevant legislation
budget allocations
warranties and service information.

Appropriate person(s) may include:
clients
site managers, project managers
engineers and technicians
technical experts
line managers/supervisors
colleagues, security consultants
regulatory personnel.

Organisational requirements may relate to:
legal and organisational operational policies and procedures
operations manuals, induction and training materials
insurance policy agreements
client and organisational confidentiality requirements
organisational goals, objectives, plans, systems and processes
employer and employee rights and responsibilities
own role, responsibility and delegation
quality and continuous improvement processes and standards
client service standards
defined resource parameters
OHS policies, procedures and programs
emergency and evacuation procedures
duty of care, code of conduct, code of ethics
access and equity policy, principles and practice
records and information systems and processes
communication channels and reporting procedures.

Tools and equipment may include:
computer, software, back-up disks
test equipment (multimeter)
hand tools, fixing tools, crimp tools, IDC tools
strippers, router, file, drill, power saw
lockpick, pick gun, followers

glass break tester, spirit level
soldering iron, welder
ladder, hoist, drop sheet, batteries
personal protective equipment
communications equipment.

Materials may include:

computer disks
circuit board cleaner
computer cables/leads
software
interface PCBs.

Personal protective clothing and equipment may include:

masks, safety glasses, head protection, ear muffs
safety boots, knee pads
gloves
witches hats, flashing lights
warning signs and tapes
fire extinguisher
first aid kit.

Risks and hazards may include:

non-compliance with building codes and regulations
exposed electrical wiring
manual handling
chemical hazards (battery corrosion)
exposure to:
asbestos
dust
noise
live power
vermin
water
glass fibre
building debris
natural and other gas build-up.

Security equipment and systems may include:

detection devices, audible/visual warning devices
cameras, monitors and control equipment
control panels, intercoms
wireless equipment, car alarms
electronic readers, electronic recognition controls
locks and locking systems
grills, lighting, boom gates, turnstiles
bank pop-up screens
smoke detection devices
electric/mechanical fire safety and fire locking systems
power supplies, batteries
security doors and door controls.

Security systems may be:

electronic
mechanical
computerised
procedural.

Site access and specific site requirements may relate to:
access and egress points, time of access
access codes, keys, passes, security clearances
union requirements
OHS requirements
building codes and regulations
heritage listings
noise control.

Safe operating practices may include:
working safely around electrical wiring, cables and overhead power lines
working safely around tools and equipment
hazard recognition
emergency procedures
awareness of electrical hazards
following confined spaces procedures
administering first aid.

Faults may be:
electronic, mechanical, procedural
software related
due to operational misuse
environmental
due to previous installation.

Operational data may be found in:
central monitoring station records
maintenance documentation
manufacturer's specifications
visual inspections
software records
back-ups.

Relevant information may include:
site variables:
equipment/system usage
environmental conditions
building structures
client habits

historical information of past performance
operational data.

Inspections may involve:
a visual inspection of:
equipment/system malfunctioning
parts and components
mechanisms
connections

using computer tools
client demonstration
environmental assessment.

Systematic fault-finding may involve:
using a methodical approach
progressively isolating fault
using testing equipment
verifies continued existence of problem
reviews all available information
identifies fault in shortest time possible.

Documentation may detail:
completion of work log
equipment/system problem
fault diagnosis
warranty conditions and allowances
recommendations for repair
circuit diagrams and flow charts
keying plans.

Applicable legislation, **codes and national standards may relate to**:
compliance with Australian building codes and regulations
compliance with Australian Communications Authority (ACA) cabling standards
relevant Commonwealth/State/Territory legislation which affect organisational operation:
Occupational Health and Safety and safe work practices
environmental issues
equal employment opportunity
industrial relations
anti-discrimination and diversity

licensing arrangements
Australian Standards, quality assurance and certification requirements
relevant industry Codes of Practice
trade practices, award and enterprise agreements
privacy requirements and related legislation.

The Range of Variables provides information about the context in which the unit of competency is carried out. It allows for different work practices and work and knowledge requirements as well as for differences between organisations and workplaces. The following variables may be present for this particular unit:

Work order information may relate to:
work schedules
completion dates
job requirements and tasks
specific client requirements
access to site and specific site requirements
resource requirements
OHS requirements
compliance with relevant legislation
budget allocations

warranties and service information.

Appropriate person(s) may include:

clients
site managers, project managers
engineers and technicians
technical experts
line managers/supervisors
colleagues, security consultants
regulatory personnel.

Organisational requirements may relate to:

legal and organisational operational policies and procedures
operations manuals, induction and training materials
insurance policy agreements
client and organisational confidentiality requirements
organisational goals, objectives, plans, systems and processes
employer and employee rights and responsibilities
own role, responsibility and delegation
quality and continuous improvement processes and standards
client service standards
defined resource parameters
OHS policies, procedures and programs
emergency and evacuation procedures
duty of care, code of conduct, code of ethics
access and equity policy, principles and practice
records and information systems and processes
communication channels and reporting procedures.

Tools and equipment may include:

computer, software, back-up disks
test equipment (multimeter)
hand tools, fixing tools, crimp tools, IDC tools
strippers, router, file, drill, power saw
lockpick, pick gun, followers
glass break tester, spirit level
soldering iron, welder
ladder, hoist, drop sheet, batteries
personal protective equipment
communications equipment.

Materials may include:

computer disks
circuit board cleaner
computer cables/leads
software
interface PCBs.

Personal protective clothing and equipment may include:

masks, safety glasses, head protection, ear muffs
safety boots, knee pads
gloves
witches hats, flashing lights

warning signs and tapes
fire extinguisher
first aid kit.

Risks and hazards may include:
non-compliance with building codes and regulations
exposed electrical wiring
manual handling
chemical hazards (battery corrosion)
exposure to:
asbestos
dust
noise
live power
vermin
water
glass fibre
building debris
natural and other gas build-up.

Security equipment and systems may include:
detection devices, audible/visual warning devices
cameras, monitors and control equipment
control panels, intercoms
wireless equipment, car alarms
electronic readers, electronic recognition controls
locks and locking systems
grills, lighting, boom gates, turnstiles
bank pop-up screens
smoke detection devices
electric/mechanical fire safety and fire locking systems
power supplies, batteries
security doors and door controls.

Security systems may be:
electronic
mechanical
computerised
procedural.

Site access and specific site requirements may relate to:
access and egress points, time of access
access codes, keys, passes, security clearances
union requirements
OHS requirements
building codes and regulations
heritage listings
noise control.

Safe operating practices may include:
working safely around electrical wiring, cables and overhead power lines
working safely around tools and equipment
hazard recognition

emergency procedures
awareness of electrical hazards
following confined spaces procedures
administering first aid.

Faults may be:
electronic, mechanical, procedural
software related
due to operational misuse
environmental
due to previous installation.

Operational data may be found in:
central monitoring station records
maintenance documentation
manufacturer's specifications
visual inspections
software records
back-ups.

Relevant information may include:
site variables:
equipment/system usage
environmental conditions
building structures
client habits

historical information of past performance
operational data.

Inspections may involve:
a visual inspection of:
equipment/system malfunctioning
parts and components
mechanisms
connections

using computer tools
client demonstration
environmental assessment.

Systematic fault-finding may involve:
using a methodical approach
progressively isolating fault
using testing equipment
verifies continued existence of problem
reviews all available information
identifies fault in shortest time possible.

Documentation may detail:
completion of work log
equipment/system problem
fault diagnosis
warranty conditions and allowances

recommendations for repair
circuit diagrams and flow charts
keying plans.
Applicable legislation, **codes and national standards may relate to**:
compliance with Australian building codes and regulations
compliance with Australian Communications Authority (ACA) cabling standards
relevant Commonwealth/State/Territory legislation which affect organisational operation:
Occupational Health and Safety and safe work practices
environmental issues
equal employment opportunity
industrial relations
anti-discrimination and diversity

licensing arrangements
Australian Standards, quality assurance and certification requirements
relevant industry Codes of Practice
trade practices, award and enterprise agreements
privacy requirements and related legislation.

Unit Sector(s)

Not applicable.