Australian Government

Department of Education, Employment and Workplace Relations

ICANWK502A Implement secure encryption technologies

Release: 1

ISC INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICANWK502A Implement secure encryption technologies

Modification History

Release	**Comments**
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to ensure secure encryption is selected, implemented and monitored in an information and communications technology (ICT) network, either locally or both.

Application of the Unit

This unit applies to information technology (IT) professionals who may select, implement and monitor a secure encryption environment in any size enterprise. The encryption system may include local file encryption and encryption across computer networks.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	**Performance Criteria**
Elements describe the essential outcomes of a unit of competency.	*Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.*

Elements and Performance Criteria

1. Determine encryption methods	1.1 Analyse enterprise data ***security*** requirements 1.2 Create a new or review an existing ***security plan*** to determine appropriate ***encryption*** methods 1.3 Review a range of ***encryption technologies*** and rank the most appropriate options 1.4 Assess the costs associated with each encryption option 1.5 Document encryption options and costs and forward to ***appropriate person*** for decision
2. Implement encryption	2.1 Apply encryption technologies to the enterprise system 2.2 Analyse effect of encryption technologies on ***user*** roles and responsibilities 2.3 Inform user of new encryption technologies and effect it has on their responsibilities
3. Monitor encryption	3.1 Analyse implementation of the encryption technologies, confirming function and performance 3.2 Review help-desk records for problems concerning implementation and take appropriate action 3.3 Review system logs for encryption issues and compromises 3.4 Document encryption issues and compromises, notifying appropriate person

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- analytical skills to:
  - analyse enterprise data security requirements and help-desk records
  - monitor and assess encryption systems
  - review a range of encryption software and tools
  - review security plan and conduct a detailed survey, including effect on user
  - review system security logs for breaches
- communication skills to:
  - convey and clarify complex information
  - liaise with users and clients
- literacy skills to:
  - create and interpret a data security analysis report
  - interpret an enterprise security plan
  - interpret and prepare technical documentation that includes encryption options and costs
- numeracy skills to make estimates and comparison of costs (cost-benefit analysis)
- planning and organisational skills to analyse effect on user and plan for organisational change
- problem-solving skills to troubleshoot, debug and correct connectivity and security issues
- research skills to:
  - assess and compare encryption options
  - determine data security threats, risks and countermeasures
- technical skills to:
  - develop enterprise policy and procedures
  - implement best practice encryption systems
  - implement local area network (LAN) or wireless local area network (WLAN), virtual private network (VPN) or wide area network (WAN) solutions
  - monitor encryption system for issues and compromises
  - test and prove function of chosen encryption system
  - undertake a network security risk assessment.

Required knowledge

- certificate-related infrastructure (certificate authorities, registration authorities, repository services)
- common asymmetric key algorithms and their usage
- common symmetric key algorithms and their usage, such as:
  - advanced encryption standard (AES)
  - data encryption standard (DES)
  - triple data encryption algorithm (triple DES)

  - Blowfish
- encryption strength
- encryption types (public key, secret key, hash key)
- functions and features of:
  - access control permissions
  - digital signatures
  - symmetric encryption, asymmetric encryption and one-way encryption
  - timestamps
- one-way message digests, such as message digest algorithm 5 (MD5) and secure hash algorithm (SHA)
- public key infrastructure (PKI), pretty good privacy (PGP) and GNU Privacy Guard (GnuPG)
- replay security
- sources of security threats, including eavesdropping, data interception, data corruption, data falsification and authentication issues
- transmission control protocol or internet protocol (TCP/IP) protocols and applications
- security problems and challenges that arise from organisational issues
- wired equivalent privacy (WEP), wi-fi protected access (WPA) and wi-fi protected access 2 (WPA2).

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • analyse enterprise data security requirements • create new or review existing security plan to determine the appropriate encryption methods • rank and document appropriate encryption methods • implement encryption systems informing users of any affects • monitor and document encryption issues and compromises notifying appropriate person.
Context of and specific resources for assessment	Assessment must ensure access to: • site where encryption installation may be conducted • live network • servers • encryption software • encryption tools • appropriate learning and assessment support when required. Where applicable, physical resources should include equipment modified for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • review of security analysis and planning report that outlines enterprise security requirements and security plan, including challenges faced and how these were addressed • evaluation of documentation demonstrating review of suitable encryption systems, ranking the most appropriate • verbal or written questioning to assess candidate's knowledge of encryption types, algorithms, functions and features • direct observation of candidate performing tasks required to successfully implement and monitor a chosen encryption system.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate.

	Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Security may include:	• access policies • data protection requirements: • encryption • permissions • secure remote access • tamper identification • user authentication and control • information rights management • roles and site permissions.
Security plan may include:	• enterprise processes • enterprise requirements • enterprise security policies • enterprise work practices and procedures • security analysis report.
Encryption may include:	• asymmetric public-key ciphers • digital signatures • PGP • PKI • PKZIP • Rivest, Shamir and Adelman (RSA) • secure shell (SSH) • secure socket layer (SSL) • symmetric ciphers.
Encryption technologies may include:	• Blowfish Advanced CS • Cryptainer LE • GnuPG • inbuilt operating system file encryption systems • new PKI • open VPN • PGP.
Appropriate person may include:	• authorised business representative • client • supervisor.

User may include:	- department within the enterprise - person within an enterprise department - third party.

Unit Sector(s)

Networking