



Australian Government

Department of Education, Employment and Workplace Relations

ICAWEB408A Ensure basic website security

Release: 1

ICAWEB408A Ensure basic website security

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to provide basic website server and protocol security appropriate to the level required by an organisation.

Application of the Unit

This unit applies to web maintenance staff who are required to ensure that a website meets basic security requirements.

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
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>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.</i>

Elements and Performance Criteria

1. Determine business security requirements	1.1 Identify level of security required based on the business and commercial intent of the website 1.2 Identify whether password protection is needed for the site or part of the site 1.3 Decide minimum or maximum password protection solutions based on business requirements
2. Ensure web server security	2.1 Ensure that web server password is obscure and non-traceable 2.2 Install and maintain an effective intrusion detection system according to business requirements 2.3 Ensure that user accounts have only the required permissions on the server 2.4 Ensure that interpreters' programs that run common gateway interfaces (CGIs) are not stored in the CGI-bin directory 2.5 Ensure that web forms check data before passing it to the server
3. Ensure protocol security	3.1 Protect fixed internet connection and internet protocol (IP) address 3.2 Protect shared network resources from intrusion according to business requirements 3.3 Ensure that personal computer (PC) protocols and preferences follow security protocols 3.4 Disable control protocol or internet protocol (TCP/IP) bindings for file and printer sharing 3.5 Ensure that network basic input/output system (NetBIOS) over TCP/IP is disabled

Required Skills and Knowledge

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

Required skills

- communication skills to liaise with internal and external personnel on technical, operational and business-related matters
- numeracy skills to:
 - take test measurements
 - interpret results
 - evaluate performance
- planning and organisational skills to plan, prioritise and monitor own work
- research skills to interrogate vendor databases and websites
- technical skills to:
 - write hypertext markup language (HTML)
 - write JavaScript and VBScript.

Required knowledge

- client business domain, including client organisation structure and business functionality
- current industry-accepted hardware and software products
- desktop applications and operating systems as required
- firewall functionality
- hypertext transfer protocol (HTTP) daemons
- secure socket layer (SSL) protocol
- security patches
- specific purpose security computers acting as bastion hosts
- web-server operating systems.

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: • identify password protection solutions • install and maintain intrusion detection system • manage protocol security.
Context of and specific resources for assessment	Assessment must ensure access to: • a basic website • web servers • 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: • direct observation of candidate installing and testing website security system • verbal or written questioning to determine candidate's knowledge of: • client business requirements • industry website security standards • appropriate software and hardware to implement security on a website • evaluation of candidate's website security documentation.
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.

<i>Business requirements</i> may refer to:	• application • business • network • people in the organisation • system.
<i>Server</i> may include:	• application or web servers • building environmental assessment (BEA) weblogic servers • email servers • file and print servers • firewall servers • file transfer protocol (FTP) servers • IBM VisualAge and WebSphere • Novell Directory Services (NDS) servers • proxy or cache servers.
<i>Intrusion detection system</i> may include:	• Cisco • HP • Symantec • Tripwire.
<i>User</i> may include:	• department within the organisation • person within a department • third party.
<i>Connection</i> may include:	• asymmetric digital subscriber line (ADSL) • cable • fixed line.
<i>Network</i> may include:	• data • internet • large and small local area networks (LANs) • national wide area networks (WANs) • private lines • use of the public switched telephone network (PSTN) for dial-up modems only • voice.
<i>Security protocols</i> may	• data over cable service interface specification

include:	• domain name system security extensions • IEEE 802.11 Protocol standard for secure wireless local area network products • internet protocol security (IPSec) • point-to-point network tunnelling protocol (PPTP)/Layer 2 tunnelling protocol (L2TP) • secure electronic transactions • secure multipurpose internet mail extensions • secure shell • SSL and transport layer security.
----------	---

Unit Sector(s)

Web