

Training Package	Information Technology ICA99	Unit Code
Title:	Maintain system integrity	ICAITS017B
Unit Descriptor	This unit expresses the competency required to protect and secure stand-alone or client server environments.	HSC Indicative Hours: 15
Field/Stream	Support Information Technology	
Related Competency Standards	The project life cycle and the IT methodology employed will determine which particular units of competency are relevant to this unit, some include the Project Management, Implementation, Use, Documentation and Teamwork functional areas.	

Key Competencies							
Collect, Analyse, and Organise Information	Communicate Ideas and Information	Plan and Organise Activities	Work with Others and in Teams	Use Mathematical Ideas and Techniques	Solve Problems	Use Technology	Cultural Understandings
2	1	2	1	1	1	2	1

Related learning for the HSC	Resources that may be used for in training and assessment for this unit
<p>Students may draw on skills and knowledge developed in other studies to achieve competency in this unit. This can include:</p> <ul style="list-style-type: none"> • Systems Design and Development • Information Processes and Technology 	<ul style="list-style-type: none"> • Non-endorsed materials for ICAITS017B • National Information Technology Module ITH201 – Computer Administration • Computer manuals and tutorials • Materials developed by Registered Training Organisations • Various commercially produced materials including textbooks and computer tutorials

Training Package	Information Technology ICA99	Unit Code
Title:	Maintain system integrity	ICAITS017B
Unit Descriptor	This unit expresses the competency required to protect and secure stand-alone or client server environments.	HSC Indicative Hours: 15
Field/Stream	Support Information Technology	
Related Competency Standards	The project life cycle and the IT methodology employed will determine which particular units of competency are relevant to this unit, some include the Project Management, Implementation, Use, Documentation and Teamwork functional areas.	

Element of Competency	Performance Criteria	Underpinning Skills and Knowledge	Evidence Requirements	HSC Requirements
1. Carry out file maintenance	<ol style="list-style-type: none"> File back-ups are carried out Back-ups are determined and stored according to organisational guidelines Records or back-up are maintained 	<ul style="list-style-type: none"> Software copyright responsibilities A broad knowledge base incorporating some theoretical concepts of system performance Broad knowledge of maintenance procedures A broad knowledge base of inventory procedures 	<p>Critical aspects of assessment</p> <p>Assessment must confirm the ability to protect and secure stand alone or networked client server environments and operating systems according to system maintenance procedures.</p> <p>Undertaking file back-up, restore, delete and archive are carried out according to back-up and restore procedures.</p>	<p>Key Terms and Concepts</p> <ul style="list-style-type: none"> backup and restore policies and procedures virus protection policies and procedures copyright backup media file security file attributes auditing file extensions and their associations

Element of Competency	Performance Criteria	Underpinning Skills and Knowledge	Evidence Requirements	HSC Requirements
2. Carry out virus scanning	<ol style="list-style-type: none"> 1. Virus protection is maintained 2. Detected viruses are reported to supervisor and are removed 	<ul style="list-style-type: none"> • A broad knowledge base incorporating some theoretical concepts of restore procedures • A broad knowledge base of storage and retrieval guidelines • A broad knowledge base incorporating some theoretical concepts of operating systems • Current industry accepted hardware and software products with broad knowledge of general feature and capabilities and detailed knowledge in some areas • A broad knowledge base incorporating some theoretical concepts of diagnostic tools • A broad knowledge base of current viruses and protection methods 	<p>Interdependent units of assessment</p> <p>This unit may be assessed with any of the following: ICAITU019B, ICAITS025B, ICAITS012A, ICAS021B, ICAITS020B, ICAITB002, ICAITS031B. The interdependence of units of competency for assessment will vary with the particular project or scenario.</p>	<p>Learning experiences for the HSC must include:</p> <ul style="list-style-type: none"> • the backup (partial and full) and restore of computer files • the use of virus scanning software • interpreting a backup policy • changing file attributes on personal files • stacking files in nominated locations • interpreting an audit log file • safely removing programs from a computer
3. Follow software copyright procedures	<ol style="list-style-type: none"> 1. Software licenses are monitored 2. Illegal software is determined 3. Illegal software is reported to supervisor 			

Element of Competency	Performance Criteria	Underpinning Skills and Knowledge	Evidence Requirements	HSC Requirements
4. Licensed software is determined	<ol style="list-style-type: none"> 1. Licensed software is determined 2. Records of license number and location are maintained 3. Personal computers and networks are checked for illegal software 4. Illegal software is reported to supervisor 	<ul style="list-style-type: none"> • Plain English literacy and communication skills in relation to the presentation of information • Basic diagnostic skills in relation to system integrity • Questioning and active listening in regard to clarifying instructions • Basic analytical skills in relation to system integrity • Problem-solving skills for a defined range of predictable problems • Problem solving in regard to known problems in routine procedures • Research skills for identifying broad features of current viruses and best practice in virus protection 		
5. Restore system back-up	<ol style="list-style-type: none"> 1. Back-ups are restored 2. Restore procedures are determined according to the organisational guidelines 3. Restore is carried out under supervisor instruction 4. Restore carried out is recorded according to the organisational guidelines 			

Resources	Competency is to be assessed through practical demonstration or performance. Competency can also be demonstrated in a simulated environment. Peers and supervisors for obtaining information on the extent and quality of the contribution made.
Consistency	Competence in this unit needs to be assessed using formative assessment to ensure consistency of performance in a range of contexts.
Context	Work is carried out under direct supervision. An individual demonstrating these competencies would be able to: <ul style="list-style-type: none"> • demonstrate knowledge by recall in a narrow range of areas • demonstrate basic practical skills, such as the use of relevant tools • perform a sequence of routine tasks given clear direction, and • receive and pass on messages/information.
Range of Variables	
Variable	Scope
Hardware	Variables may include, but are not limited to: personal computers, networked systems, tools to perform back-ups such as tapes, streamers, floppy disks.
Software	Software application/operating system with system security functions.
Organisation	Variables may include, but are not limited to: security procedures; backing-up procedures; virus removal procedures; software license documentation; reporting of illegal software; restore procedures.
Literacy skills	In regard to reporting and recording organisational documentation.
Client user	May be a department within the organisation or a third party. Consequently, the relationship and ease of access will vary.
Documentation and reporting	Audit trails, naming standards, version control.
OH & S standards	As per company, statutory and vendor requirements. Ergonomic and environmental factors must be considered during the demonstration of this competency.
Organisational standards	May be based upon formal, well documented methodologies or non-existent. For training delivery purposes, best practice examples from industry will be used.