Australian Government

Assessment Requirements for ICTSAS206 Detect and protect from spam and destructive software

Release: 1

Assessment Requirements for ICTSAS206 Detect and protect from spam and destructive software

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

Evidence of the ability to:

- install virus protection software and updates
- schedule virus protection software to run on a regular basis
- remove common destructive software
- identify common spam types and take appropriate action.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- describe spam and virus intrusions and identify appropriate remedial actions
- identify the types of protective applications used against viruses and spam
- identify the operating systems supported by the organisation
- identify the common components of computer hardware that may be affected by spam.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the systems administration and support field of work and include access to:

- sites with a representative range of computer hardware, application software and operating systems
- current antivirus and anti-spam software
- technical records, vendor documentation, enterprise procedures and guidelines.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet - https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2