CANTERBURY
TECHNICAL INSTITUTE

ASSESSMENT

ICT50715
Diploma of Software Development

Network Security

Assessment Code:

DITS-NETSEC-1

ICTNWK511 - Manage network security

Assessment Overview

This assessment deals with the skills and knowledge required to implement and manage security functions throughout a network.

Version 1.0 - 2017
CRICOS Code – 02938M RTO No: 31645

Information for Candidate:

- All work is to be entirely of the candidate.

General Information for this assessment:

- Read the instructions for each question very carefully.
- Be sure to PRINT your FULL name & LAST name in every place that is provided.
- Short questions must be answered in the spaces provided.
- For those activities requesting extra evidence such as: research reports, ESSAY reports, etc. The student must attach its own work formatted in double space, Arial 12 pts.
- All activities must be addressed correctly in order to obtain a competence for the unit of competency.
- If the candidate doesn't understand the assessment, they can request help from the assessor to interpret the assessment.

Re-assessment of Result & Academic Appeal procedures:

If a student at CTI is not happy with his/ her results, that student may appeal against their grade via a written letter, clearly stating the grounds of appeal to the Deputy Principal. This should be submitted after completion of the subject and within fourteen days of commencement of the new term.

Re-assessment Process:

- An appeal in writing is made to the Deputy Principal providing reasons for re-assessment /appeal.
- Deputy Principal will delegate another faculty member of CTI to review the assessment.
- The student will be advised of the review result done by another assessor.
- If the student is still not satisfied and further challenges the decision, then a review panel is formed comprising the lecturer/trainer in charge, the Deputy Principal and the Director of Student Services OR if need be an external assessor.
- The Institute will advise the student within 14 days from the submission date of the appeal. The decision of the panel will be deemed to be final.
- If the student is still not satisfied with the result, the he / she has the right to seek independent advice or follow external mediation option with CTI's nominated mediation agency.
- Any student who fails a compulsory subject or appeals unsuccessfully will be required to re-enrol in that subject.

The cost of reassessment will be borne by the Institute. The external assessor will base his/her judgement based on principles of assessment. These principles require assessment to be reliable, fair, practical and valid.

Academic Appeals

- If you are dissatisfied with the outcome of the re-evaluation process, you have a right to appeal through CTI's complaint / grievance protocol.
- The notice of appeal should be in writing addressed to the Deputy Principal and submitted within seven days of notification of the outcome of the re-evaluation process.
- If the appeal is not lodged in the specified time, the result will stand and you must re-enrol in the unit.
- In emergency circumstances, such as in cases of serious illness or injury, you must forward a medical certificate in support of a deferred appeal. The notice of appeal must be made within three working days of the concluding date shown on the medical certificate.
- The decision of Deputy Principal will be discussed with the PEO and will be final.
- Student would then have the right to pursue the claim through an independent external body as detailed in the students' complaint / grievance policy.

Submission Details:

The assessment task is due on trainer provided date. Any variations to this arrangement must be approved in writing by your assessor. Submit this document with any required evidence attached. See specifications below for details

Performance objective

The candidate must demonstrate skills, knowledge and understanding and promote the use and implementation of innovative work practices to effect change, as states the unit of competency **ICTNWK511**. Throughout this program, you are to demonstrate knowledge in:

- Australian Computer Society Code of Ethics.
- Federal and state or territory legislation and policy relevant to an IT environment relating to:
  access and equity, copyright and intellectual property and OHS.
- Privacy.
- Organisational communication processes and procedures.
- Organisational requirements for customer service.

And skills in:

- Communication skills to liaise with internal and external personnel on ethical and privacy, operational and business-related matters.
- Learning skills to update personal ethical and privacy knowledge through professional development literacy skills to apply standards and legislation to policy and procedure development and monitoring.
- Planning and organisational skills to plan, prioritise and monitor own work.
- Research skills to gain and maintain current industry privacy and ethical information.
- Technical skills to perform application and system security and storage management.

Assessment description:

You will undertake **computer based test** based on class lectures and activities in this Practical Activity.

Procedure:

1 You will need to follow instructions below and address all activities required.
2 This is an individual activity where each candidate will be assessed individually;
3 Complete all activities and submit assessment evidence (including these papers) to your assessor the date specified above (see submission details).
4 Referencing: All findings from the internet or other sources must be referenced as per standards laid by APA referencing guide at: http://www.usq.edu.au/library/help/referencing/apa

Specifications/Conditions:

Your assessor will be looking for evidence of:

- Analyse legislation and standards relating to professional conduct and privacy in the IT industry
- Contribute to the development of a code of ethics and monitor the workplace to ensure code of ethics is being applied and is appropriate
- Contribute to the development of a privacy policy and monitor the workplace to ensure the policy is being applied and is appropriate.
- Relevant organisational policies, legislation and standards documentation.
- Industry codes of practice.

Assessment Details

Network Security Threat Assessment and Support Plan

Task 1: Threat and analyse report for network security.

Complete a report that addresses the following topics:

- Why is network security important?
- Why network attacks occur and from whom?
- Types of network attacks, give at least three examples.

Your report must contain:

1) The Tittle page must include the subject of the report, who the report is for, who the report is by and the date of submission.

2) ABSTRACT — An abstract is usually 100 to 200 words and should include the following:

    - Why the report has been written (i.e. what question or problem is it addressing?)
    - How the study was undertaken
    - What the main findings were
    - What the significance of the findings are.

    Be specific and precise so that the reader can get a good understanding of the main points without having to read the whole report. The abstract should be on a separate page with the centred heading ABSTRACT in capitals. It is usually written in a single paragraph with no indentation.

3) TABLE OF CONTENTS — The Table of Contents should be on a separate page. It helps the reader to find specific information and indicates how the information has been organised and what topics are covered. The table of contents should also include a list of figures and a list of tables if any are used in the report.

4) INTRODUCTION — The Introduction has three main components.

    4.1. The Background which describes what is necessary.
    4.2. The Purpose which defines what the study is to achieve.
    4.3. The Scope which outlines any limitations imposed on.

5) Points of Discussion - Need to discuss the points from different angel as you think.

6) CONCLUSIONS —The Conclusions should be as brief as possible. They should be presented in descending order of importance and should not suggest action. Conclusions should be free from speculation (i.e. ideas for which you have presented no evidence), have no new thoughts or references introduced and contain no further discussion of points raised.

Task 2: Security plan and response.

Create a security plan that covers the following criteria:

- Two scenarios of a network attack.
- Counter measures that reduce the risk of the attacks for the previous scenarios.
- Policies for the acceptable use of the network.
- Response plan in the event of a successful attack, based on the previous scenarios.

Assessment Submission Details

This assessment requires the following evidence:

Required documentation to be included in a single compressed archive (**ZIP** or **7z**) file as follows:

- Threat and analyse report for network security
- Security plan and response document.
- Any other relevant documents/source code/reports for this assessment.

Submit the compressed archive electronically via edRES submissions section or if otherwise instructed by your assessor/instructor.