**All Due: 6/6/19**

**Unit 2: Networking – Assignment 2**

**Part 1 Design efficient networked systems**

Should be complete already with evaluated design feedback from me. See my website for further documentation. CHECK ALL TASKS COMPLETED ON ASSIGNMENT BRIEF.

**M3** Install and configure network services and applications on your choice.  
**D2** Design a maintenance schedule to support the networked system.

**Part 2 Implement, test and diagnose networked systems**

**Implement a networked system based on your prepared design.**

Using your design plan as a guide configure windows server with domain services and test that users can log in using Windows 10.

**Conduct verification with e.g. Ping, extended ping, trace route, telnet, SSH, etc.**

Screenshot the use of ping (e.g. ping 192.168.1.1), traceroute (tracert 192.168.1.1).

Use telnet to test for ports open (e.g. telnet 192.168.1.100 80).

Main email port: SMTP – 25

## Main internet port: HTTP - 80

**Record the test results and analyse these against expected results.**

Create a table like below. Include everything you have installed or configured on Windows Server. Include tests at the client end to check services and features have been set up correctly. Screenshot’s ideally should be used as evidence.

|  |  |  |  |
| --- | --- | --- | --- |
| **Test** | **Expected Result** | **Actual Result** | **Problems** |
| Installation of Windows 2012 | Successful installation of NOS | Successful but had issues creating a new partition. | List issues and how you overcame them. |
| Domain created/set up | Successful domain creation of ABCMarketing.net domain |  |  |

**Investigate what functionalities would allow the system to support device growth and the addition of communication devices.**

Think about the strengths and weakness of the network and its creation.

**M4** Recommend potential enhancements for the networked systems.

**Discuss the significance of upgrades and security requirements in your recommendations.**

**D3** Use critical reflection to evaluate own work and justify valid conclusions.

**Unit 5 Security – Assignment 2**

See the assignment brief for further information.

**Part 1 – Theory Report. (2,000–2,500 words)**

See my LO3 PowerPoint and assignment brief for help. In addition:

**Discus stakeholders such as:**

* Management
* Resource owners (Hardware and software)
* System users (Computer Users, Data Entry Staff, Data Processors, Information Collectors etc)
* Human Resources
* External Representatives (Clients, external contractors)
* Legal & Regulatory
* Security Specialists
* Public Relations

A good starting point for this:

<https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1124&context=ism>

**List and discuss elements needed for a disaster recovery plan:**

<https://www.ontrack.com/uk/blog/top-tips/writing-a-disaster-recovery-plan-for-your-small-business-free-template/>

**Part 2 – Design and implement a security policy. (Policy document)**

See example policies and templates on my website. Use a combination of these to develop your own policy. Write a short justification for your policy and add it to the end of your part 1 report.

Include your security policy in the appendix of this assignment.

**Part 3 – Evaluate tools used in the security policy. (250–500 words)**

**Consider group policy within windows server including access and service rights along with password policies. Good article to get started:**

<https://sourcedaddy.com/windows-7/configuring-security-policies.html>