# Secure Remote Access Networks Assignment

## Customer Overview

Company ACME is a small private company that currently has 120 employees over two floors in a multi-story office building in Melbourne. ACME has currently two divisions within its parent company. One division is a property management group; another is in commercial real estate. Profits for the company are around 1 million dollars annually.

## Scenario Overview



Main Offices

Primary Datacentre

Secondary Datacentre



SwitchA

SwitchB



Leased Rack

Servers



Servers





ACME has leased two racks in two separate small multi-tenant datacentres. In the primary datacentre, they have a rack containing a series of servers for storing their data, running their enterprise applications, and their company email. There also a series of public http servers in a virtual server farm in a DMZ. The secondary Datacentre provides full redundancy. Access to the internet comes off the Firewall in the Datacentres. ACME has full control of the equipment used in the Datacentres.

The company has problems in that general staff have been accessing data between the two divisions, which should not occur. Contractors and Salespeople who come into the Company need minimal access to the company’s servers and the internet but currently have access to everything. An audit has found that staff has been using the company email for personal things and has been downloading inappropriate material from the Internet.

## Growth

The business is intending to grow by about 30 – 50 employees and intends to lease a third floor in the main office. This will be a new Construction Division business unit.

The company also wants to provide wireless access across the three floors.

# Assignment

The company currently does not have any Security Policies.

The devices that the company has does not really matter, as the assignment is to create general security policies that would assist this company in becoming cybersecurity aware and to protect themselves. The devices themselves would be addresses in the technical documents as part of the security package.

Task 1: Identify potential Network Security Policies **(35%)**

Identify key security polices with a brief description of that policy that you think could benefit ACME.

You need to do some research and find out what goes into a security policy.  There are many security policies in which could be used by ACME. You need to briefly identify between six and eight potential security polices and give a brief description of each.

The purpose of this task is identifying what policies needs to be formulated. These could include things like extranet policy, minimum requirements for network access policy, network access standards, router and switch security policy, and server security policy. Students will need to identify organisational assets and the way they are used or misused, to create effective security policies.

Task 2: Create security policies for two of the sections you have listed. **(35%)**

Here you will create two full policies out of your recommended policies listed in Task 1.

Security policies are usually broken down into sections including, Overview, Purpose, Scope, Policy, Policy Compliance, Related standards, Definition and terms, and Revision History

There are hundreds of security policy templates available on the Internet through places like SANS. You may use the templates as a guideline, but it must be specific to ACME. You are submitting this via TurnItIn, so just trying to copy a policy you find somewhere will not be tolerated and will result in plagiarism.

Task 3: Create a “Network Equipment Security Guidelines” Document as a supplement to a Basic Security Policy. **(20%)**

You are creating a very specific guidelines covering ACME’s Networking equipment. Guidelines are a step down from policies. You are NOT the networking team doing the configuration of the specific devices that ACME is using. Exactly what they use is not important. You are to provide detailed security guidelines that the networking team will use in the deployment and configuring of the networking devices.

Guidelines are a list of suggestions on how to do things more efficiently and securely. They are similar to standards but are not usually mandatory. Guidelines are often also called Best Practices.

You can find information at places like NIST Computer Security Resource Center or NSA Security Configuration Guides.

Formatting and Content **(10%)**

This will be based on things like table of content, page numbering, title page, consistent formatting and the like.

The Academy information on this assignment content is found in Chapter 1 and 11.

The idea of this assessment is for you to seek and learn.

This is to be done in groups of three or four. You are to self-enrol into groups in Canvas. The Masters students can keep the same group they formed for their case study but must recreate the group in Canvas.