My part:

Here I am going to give a detailed Network Security Policy regarding Wireless Communication Policy using the Free to Use SANS Template as a basis (and also the wireless communication policies of “College of Saint Mary” and “William And Mary”) and creating a suitable and robust policy for ACME to use:

**1. Overview**

Nowadays, there has been a huge increase in the number of smartphones and tablets used by people, leading to almost all companies allowing their employees to access company resources on their own device via BYOD (Bring your own device) in order to increase work efficiency and effectiveness. This in turn has led to wireless connectivity becoming a must have in each and every organization. So, the ACME company deciding to provide wireless access across all of its floors (including the new 3rd one) is quite in line with the times.

But considering the dangers that insecure wireless configurations provide (alongside the fact that this is the company’s first setup of wireless access), the desire for a strong and effective wireless communication policy for the company is quite high.

**2. Purpose**

This policy has been made to secure and protect the information assets owned by ACME by establishing rules and procedures regarding wireless access to company resources. This ensures that personnel can only gain access to those resources if either:

1. Their wireless communication devices satisfy the specified standards and protocols,
2. They have been granted an exception by the Information Security Department

Furthermore, it also ensures that the confidentiality, integrity and availability (CIA) of the informational assets in the organization are properly maintained.

**3. Scope**

All personnel affiliated with ACME (like employees from property management, commercial group or future construction group, contractors, consultants, etc.) and any third party or vendors related to ACME using any wireless communication device (like mobile phones, computers, PDA, etc) must adhere to this policy. This includes any wireless communication device that is capable of transmitting data and is either connected to or resides on  the companies’ wireless network.

**4. Policy**

All personnel using wireless devices that are either located at ACME, connecting to ACME network, or accessing resources over the company’s network must:

* Follow the standards specified in wireless communication Standard
* Use company approved authentication (Radius, Tacacs+,etc) and encryption protocol (like SHA, MD5, etc.)
* Use company approved infrastructure that are installed, supported and maintained by an approved support team
* Maintain hardware access (Like MAC address) that can be tracked
* Not interfere with other Organizations’ wireless infrastructure
* Not access or download harmful or suspicious websites or content from the internet whilst using the company network
* Not share their access with any other personnel within or outside their company
* Not impact the CIA of the information assets of the company they are accessing  in any way

Furthermore, ACME’s extremely sensitive and confidential information that is not necessary for daily business activity(like DMZ or virtual server setup) must be isolated from the corporate network and comply with *Lab Security Policy*.

Moreover, SSID set for the network must not have any information of the company in it (like name, division, id,etc) and must use proper, complex passwords (like combination of uppercase and lowercase letters, numbers, symbols,etc.)

**5. Policy Compliance**

Authorized personnel from the ACME company (like members of their Information Security Team) will periodically verify that compliance to the policy has been maintained via video monitoring, reports, audits, etc. Any employee found to have violated this policy at any time, without having explicit approval from the authorized personnel for the exception, will be subject to serious disciplinary actions, upto and including termination of employment.

**6 Related Standards, Policies and Processes**

• Lab Security Policy

• Wireless Communication Standard

**7 Definitions and Terms**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| BYOD | It is the practice of allowing the employees of an organization to use their devices for work purposes |
| CIA | It is a model designed to guide policies for information security within an organization ensuring that the confidentiality, Integrity and Availability of the information asset is maintained |
| PDA | It is a type of mobile device also known as a handheld PC |
| Radius | It is a client-server protocol that enables remote access servers, used to authenticate users |
| Tacacs+ | It is a remote authentication protocol developed by Cisco |
| SHA | It is an algorithm used to create hashes files |
| MD5 | It is a message digest algorithm that had been initially used to create hashes of files |
| MAC Address | It is a unique hardware identifier that helps identify any device on a network |
| DMZ | It is called as demilitarized zone and is basically a subnetwork that is used to  protect an organizations’ exposed outwards facing service |
| SSID | It is called Service Set IDentifier and is basically the name of the network |

**8 Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| June 2014 | SANS Policy Team | Updated and converted to new format |
| October 2022 | S M Ragib Rezwan | Updated and modified the format to be more applicable/ suitable to ACME |