Rouge Construction Wireless Communication Policy

Last Update Status: *Updated July 29,2022*

To best fit the needs and security of the employees and data of Rouge Construction, the wireless network will be on a different subnet. In doing so, the network will be able to sustain consistent traffic flow, reliability, and security. Having an overlay subnet, will prevent network congestion and give the corporation the ability to implement edge tunneling; the use of wireless switches to track roaming clients allowing them mobility.

Rouge Construction will be using the WPA3 Enterprise encryption methodology since it is considered the strongest and allows for encrypted transmissions between wireless devices and routers. It uses a 192-bit security and the 802.1x standard in order to secure wireless networks. Its security suite aligns with the recommendations of the Commercial National Security Algorithm and is used in most high-security Wi-Fi networks. Since the corporation will be using wireless technology for printing, machinery, mobile devices, workstations, etc. to transfer financial, customer, and other sensitive information, this methodology is the best option.

To proactively work against login security vulnerabilities such as user-generated credentials, brute-force attacks, lack of password complexity, unpatched security risk, and social engineering attacks, there are several practices that Rouge Construction will implement. First, it will handle consumer and employee login credentials with a cryptographic hash and salt with the most up-to-date technologies. Second, implement multi-factor authentication when possible this additional layer of the login process will prevent unauthorized users from easy access to information. Third, in the training programs for employees/staff, Rouge Construction will provide a course on password hygiene for all users such as not using personal information, using special characters, setting a minimum character limit, and limiting the amount of password reset attempts.

1. Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

2. Purpose

The purpose of this policy is to secure and protect the information assets owned by Rouge Construction. Rouge Construction provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Rouge Construction grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the Rouge Construction network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a Rouge Construction network.

3. Scope

All employees, contractors, consultants, temporary and other workers at Rouge Construction, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Rouge Construction must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Rouge Construction network or reside on a Rouge Construction site that provides wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4. Policy

4.1 General Requirements

All wireless infrastructure devices that reside at a Rouge Construction site and connect to a Rouge Construction network, or provide access to information classified as Rouge Construction Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use Rouge Construction approved authentication protocols and infrastructure.
- Use Rouge Construction approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to Rouge Construction Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the Rouge Construction network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.
- Not interfere with wireless access deployments maintained by other support organizations.

4.3 Home Wireless Device Requirements

4.3.1 Wireless infrastructure devices that provide direct access to the Rouge Construction corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

4.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Rouge Construction corporate network. Access to the Rouge Construction corporate network through this device must use standard remote access authentication.

5. Policy Compliance

5.1 Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Lab Security Policy
- Wireless Communication Standard

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- MAC address

8. Revision History

Date of Change	**Responsible**	**Summary of Change**
July 2022	Liela Pressley	**Updated**

References

Cybersecurity and Infrastructure Security Agency. (2020, May 8). Securing Wireless Networks | CISA. Retrieved July 31, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST05-003#:%7E:text=There%20are%20several%20encryption%20protocols,is%20currently%20the%20strongest%20encryption

Gupta, D. (n.d.). Login Security: 7 Best Practice for online security | LoginRadius Blog. Loginradius | Blog. Retrieved July 31, 2022, from https://www.loginradius.com/blog/identity/login-security/

The Wireless Wizards. (2004, March 1). Subnetting a wireless LAN for voice. Network World. Retrieved July 31, 2022, from https://www.networkworld.com/article/2330837/subnetting-a-wireless-lan-for-voice.html#:%7E:text=Deploying%20a%20wireless%20network%20does,than%20your%20wire%20line%20users.

WPA3 Encryption and Configuration Guide. (2022, July 28). Cisco Meraki. Retrieved July 31, 2022, from https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide