**Project Title:** CNET/SYS ADMIN FINAL PROJECT – PHASE 1

**Student name**: Joseph MUTANGANA

**Student ID:** 29061

**Course:** INSY 8211 (A)

**Lecturer:** Joshua IRADUKUNDA

**Date of submission:**

## 

## 1. Foreword

A short, personal note about your motivation, your appreciation to the professionals you interviewed, or what this project meant to you.

Example:

This project was an opportunity to explore how real companies manage their networks and systems. I thank all the professionals who agreed to share insights and experiences.

## 2. Abstract

Write this **last**, but place it here.  
It should be a brief **summary of your entire report** (1 paragraph, ~150–250 words).

It must mention:

* The objective (what you did)
* The method (interviews + research)
* Key findings (brief points)
* The significance (why it matters)

**3.** Table of Contents

Table of Contents

[1. Foreword 1](#_Toc210345288)

[2. Abstract 1](#_Toc210345289)

[4. Introduction 2](#_Toc210345290)

[5. Methodology 2](#_Toc210345291)

[6. Findings 2](#_Toc210345292)

[7. Discussion 3](#_Toc210345293)

[8. Conclusion & Recommendations 3](#_Toc210345294)

[9. References 3](#_Toc210345295)

[10. Appendices 4](#_Toc210345296)

## 4. Introduction

Define your project goals clearly:

* Objective of the project
* Scope (what areas you focused on)
* Why this project is relevant (real-world relevance)
* Short mention of methodology (details in next section)

## 5. Methodology

Break this into sub-sections:

* **Identifying Professionals**: How you found people (e.g., LinkedIn, referrals)
* **Interview Process**: How you scheduled and conducted the interviews (in-person, email, etc.)
* **Confidentiality**: Explain how you protected identities and respected sensitive info
* **Tools Used**: If you used forms, notes, recordings, etc.

## 6. Findings

a. Infrastructure Setup & Implementation

* NAT configuration (how public/private IPs are handled)
* Internet links: active/standby setup
* AD integration (on-premise with Microsoft 365)
* Tools used in system design
* Scalability and future planning

b. Daily Operational Practices

* Routine admin tasks
* System health monitoring strategies
* Troubleshooting methods (including common issues)
* Network performance optimization tools

c. Group Policies & Administrative Controls

* Password and access control policies
* Network segmentation (e.g., guest vs employee)
* Email/internet usage policies
* Account management, backup strategies, and change control
* Remote access: VPNs, mobile worker support
* AD and Group Policy management (on-prem/cloud)

d. Compliance & Security

* Compliance with ISO, NIST, or national standards
* How regulations shape internal policies
* Audit processes and enforcement methods
* Security tools and best practices

## 7. Discussion

Here you **analyze** what you learned:

* What real-world practices align with theory?
* Where did theory fall short?
* What were surprising insights?
* How do regulations shape operations?
* Any differences between companies you talked to?

## 8. Conclusion & Recommendations

Summarize:

* Key lessons learned
* What would you suggest as best practices?
* What should new sysadmins keep in mind?
* Mention how this helps bridge theory to practice

## 9. References

If you cited any:

* ISO/NIST documents
* Books or research papers
* Articles from Cisco, Microsoft, etc.

Use **APA format** (or as instructed)

## 10. Appendices

Include:

* Interview questions
* Completed sample interview forms
* Screenshots (if you did any visual mapping)
* The official confirmation email or letter