|  |  |
| --- | --- |
| A picture of a winding road and trees  Project Specification | Solomon Morongwa Moshokoa: ST10229897  Bornwise Nkateko Baloyi: ST10105509  Roandiswa Mbedzi: ST10064879  Mokgadi Mamabolo: ST10204666  WORK INTEGRATED LEARNING  Group 3  DMT2 |

**Table of Contents**

**Scope**

* Plan Scope Management
* Collect Requirements
* Define Scope
* Create WBS (Work Breakdown Structure)
* Validate Scope
* Control Scope
* Stakeholder Involvement
* Budget and Duration Management
* Addressing Challenges

**Choice and Justification**

* Why Did We Choose This Topic?
* What Do We Hope to Achieve from This Project?

**Project Description: Enhancing Network Infrastructure for Seamless Connectivity**

* Objectives
* Scope of the Project
* Stakeholders
* Budget and Timeline
* Installation and Configuration
* Anticipated Challenges
* Conclusion

**Scope**

**Plan Scope Management:** In the initial phase of our project, we'll focus on establishing a robust plan to manage the project scope effectively and this includes outlining the scope management approach, defining roles and responsibilities, and setting clear communication channels to ensure all stakeholders are aligned with the project's objectives and deliverables (Jackson, 2020).

**Collect Requirements:** To ensure seamless and secure access to the network for our 100 active users across the three main buildings and their respective lobby areas, we'll engage in comprehensive requirement gathering (Jackson, 2020). This involves understanding the specific needs of each building, assessing the wireless and wired connectivity necessities, identifying the equipment required for internet sharing, and detailing the integration of three high-speed printers in each location (Jackson, 2020).

**Define Scope:** Building upon the collected requirements, we'll define the precise scope of our project. This encompasses providing authorized personnel with secure wireless and wired network access, enabling internet sharing from the main building's high-speed cable connection, ensuring reliable connectivity for all 100 users, and seamlessly integrating the high-speed printers into the network infrastructure (Chen, 2019).

**Create WBS:** The Work Breakdown Structure (WBS) will be developed to break down the project into manageable tasks and activities. This involves tasks such as procurement of routers, access points, cables, switches, and printers, acquisition of network security software and management tools, installation and configuration of hardware and software across buildings and lobby areas, testing and optimization of network functionality and security protocols, and conducting training sessions for end-users (Chen, 2019).

**Validate Scope:** Throughout the project lifecycle, we'll continuously validate the scope to ensure that the delivered work aligns with the initially defined requirements. This involves regular reviews, user acceptance testing, and feedback mechanisms to confirm that the network access, internet sharing, connectivity, and printer integration meet the specified criteria (Chen, 2019).

**Control Scope:** Scope control mechanisms will be implemented to manage changes, prevent scope creep, and ensure that the project stays within the defined boundaries. This includes change control procedures, periodic reviews, and communication strategies to address any deviations from the agreed-upon scope (Chen, 2019).

Throughout this scope management plan, we'll involve stakeholders such as the Project Manager overseeing the project's entirety, the IT Team responsible for hardware and software installation and configuration, and the 100 end users utilizing the network and printers. The allocated budget of R1000,000 and a duration of 6 months will be meticulously managed to procure necessary hardware like routers, access points, cables, switches, high-speed printers, and essential software such as network security software, printer drivers, and management tools (Brayt, 2021). Challenges such as potential network conflicts during installation and compatibility issues between software and devices will be proactively addressed through pre-deployment network assessments, regular updates, and patches to ensure seamless integration and operation. Ultimately, this comprehensive plan aims to enhance network accessibility, security, and efficiency across our college buildings, ensuring a seamless and secure experience for all users within the specified timeframe and budget (Brayt, 2021).

Choice and justification

**WHY DID WE CHOOSE THIS TOPIC?**

We choose this topic because we have all the necessary resources to complete it and since we know very well the system we have to change, we can know what we are supposed to change in the old system so that the new system becomes better than our last system, it will be more secure and without errors that are constantly and frequently appearing and we all know what is expected of us in this topic, and unlike the other topic we all can relate to this topic. And I think it is better to create a network system of a topic all the group members understand (Brayt, 2021).

**What do we hope to achieve from this project?**

The aim is to change the entire system starting with new upgraded computers and computer software, and make a connection between those computers add a Wi-Fi, all of these devices and the printers and projector must be controlled in the main building by the IT (Information Technology) guru. elaboration within an organization or educational institution (Brayt, 2021). The design aims to provide high-speed connectivity, centralized management, and scalability to accommodate present and future technological needs. Additionally, the network design aims to enhance security by implementing measures to protect sensitive data, while also optimizing network performance through features like Quality of Service (QoS) and load balancing. Ultimately, the goal is to create a reliable and flexible network that supports the organization's objectives and growth while maintaining a high level of security and operational efficiency (Brayt, 2021).

**Project Description: Enhancing Network Infrastructure for Seamless Connectivity**

The project at hand is indispensable for ensuring 100 active users within our college have uninterrupted and secure network access. Our institution comprises three primary buildings: the main building, building 1, and Building 2. Complicating matters, each building includes a lobby area necessitating wireless network access, totalling 200 square feet. The primary objectives of this initiative revolve around providing authorized personnel with both secure wireless and wired network access, enabling internet sharing from the high-speed cable connection available in the main building, ensuring robust connectivity for our 100 users, each equipped with a computing device, and integrating three high-speed printers into each building's network infrastructure (Smith, 2022).

The scope of our project encompasses an array of tasks and activities crucial to its success. This includes procuring essential hardware such as routers, access points, cables, switches, and printers, along with acquiring imperative software like network security software, printer drivers, and management tools (Smith, 2022). The pivotal phase of installation and configuration will involve setting up hardware and software across all buildings and their respective lobby areas, followed by rigorous testing and optimization to guarantee seamless network functionality, robust security protocols, and flawless printer connectivity. Furthermore, conducting comprehensive training sessions for end-users regarding network utilization and printer operations is pivotal to ensure efficient usage (Smith, 2022).

In the realm of stakeholders, the project manager will oversee the entirety of the project, meticulously managing the budget and timelines. The IT team will be instrumental in installing and configuring the hardware and software, while the 100 end users—the college community—will heavily utilize the network and printer (Smith, 2022).

With a budget allocation of R1000,000 and a project duration set at 6 months, the procurement of necessary hardware such as routers, access points, cables, switches, and high-speed printers, alongside the acquisition of crucial software including network security software, printer drivers, and management tools, will be diligently executed. The installation and configuration team, primarily comprising IT technicians, will bear the responsibility of seamless integration and configuration (Paker, 2012).

Undoubtedly, challenges are anticipated, particularly potential network conflicts during installation and compatibility issues between software and devices. However, proactive measures have been planned, such as pre-deployment network assessments to pre-empt conflicts, and regular updates and patches to ensure seamless compatibility (Paker, 2012).

In conclusion, the project's aim is to elevate network accessibility, fortify security measures, and augment operational efficiency across our college buildings. With a comprehensive plan in place, dedicated resources allocated, and pre-emptive measures to tackle potential challenges, we are confident in achieving seamless connectivity for our users within the stipulated timeframe and budget constraints (Paker, 2012).

|  |  |
| --- | --- |
| Project name | Campus network design |
| Creation date | 06 June 2023 |
| Project charter status | Approved |
| Project sponsor signature |  |
| Proposed project start and end | 06 June 2023 – 17 November 2023 |

Project details

|  |  |
| --- | --- |
| Project description | This project is essential to ensure that all our 100 active users have seamless and secure access to the network. Our college comprises three main buildings, each with distinct requirements: the main building, Building 1, and Building 2. To make it even more complex, each building has a lobby area that requires wireless network access, spanning a total of 200 square fit, Our primary goals in this project include providing authorized personnel with secure wireless and wired access to the network, facilitating internet sharing from a high-speed cable connection available in the main building, and ensuring efficient connectivity for our 100 users, each of whom possesses a computer device. Furthermore, we have the added challenge of incorporating three large-speed printers in each building into our network infrastructure. Secure Network Access that Provide authorized personnel with secure wireless access to the network. Internet Sharing that Enable internet sharing from a high-speed cable connection available in the main building. Efficient Connectivity that Ensure the reliable connectivity for our 100 users, each equipped with a computer device. Integration of Printers that will Incorporate three high-speed printers in each building into our network infrastructure. Looking at the Scope of our project Work that includes Tasks and Activities like, Hardware Procurement that Purchase routers, access points, cables, switches, and printers. Software Acquisition that Obtain network security software, printer drivers, and management tools. Installation and Configuration that will Set up hardware and software in each building and its lobby areas. Testing and Optimization to Ensure network functionality, security protocols, and printer connectivity. Training Sessions that will |

|  |  |
| --- | --- |
|  | Conduct training for end-users on network usage and printer operations. Our project will also involve stakeholders and their role like Project Manager that Oversees the entire project, manages budget and timelines. IT Team which will Installs and configures hardware and software. End Users who our will have , the 100 college users utilizing the network and printers.  Budget and Duration Budget of R1000,000 Duration which will be complete in 6 months.  Hardware and Software that will be needed are Hardware’s being the Routers, access points, cables, switches, high-speed printers. Software being the Network security software, printer drivers, management tools. This are the tasks that are required Installation and Configuration  Team are the IT Technicians which are Responsible for installing and configuring hardware and software. Challenges and Solutions that we will be facing Challenge are Potential network conflicts during installation. Solution being Prior network assessment and testing before full deployment. Challenge are Compatibility issues between software and devices. Solution being Regular updates and patches to ensure compatibility.  Conclusion of our project is to aims and enhance network accessibility, security, and efficiency across our college buildings. With a comprehensive plan, dedicated resources, and proactive measures to address potential challenges, we are confident in achieving seamless connectivity for our users within the allocated timeframe and budget. |
| Project purpose | The purpose of our project is to aims and enhance network accessibility, security, and efficiency across our college buildings. With a comprehensive plan, dedicated resources, and proactive measures to address potential challenges, we are confident in achieving seamless connectivity for our users within the allocated timeframe and budget. |
| Project goals and objectives | Objectives and aims:  When designing a campus network system for three buildings with 100 active users, the goals and objectives must revolve around creating a |

|  |  |
| --- | --- |
|  | secure, scalable, and robust network infrastructure that meets user needs. Here are some key goals and objectives are : ⦁ Scalability: Design the network to accommodate potential growth in the number of users and devices. Ensure the network can easily scale to meet future needs without significant disruption.  ⦁ Reliability : aims to create a highly reliable network that minimizes downtime. Use redundancy and failover mechanisms to ensure continuous connectivity.  ⦁ High Performance: Ensures that the network provides high-speed, low-latency connections to support the various applications and services used by users  ⦁ Security: Implement strict security measures to protect network and user data .Use firewalls, intrusion detection systems, and encryption to protect against threats  ⦁ Segment: Network segment to separate different groups of users and sensitive data. Implement VLANs to separate traffic and improve security. |
| Project scope |  |
| Project deliverable | The main deliverable on this project will be :   * **Project Scope and Objectives:** Clearly define the scope of the project, including the goals and objectives. Specify the size of the campus, the number of users, and the types of devices that the network will support. * **Network Topology Design:**   Provide a detailed network topology diagram that illustrates the layout of the network. This should include the placement of routers, switches, access points, and other network devices. Consider redundancy and scalability in the design.   * **IP Addressing Scheme:** Define the IP addressing scheme for the campus network. Specify the |

|  |  |  |
| --- | --- | --- |
|  |  | subnets for different departments, buildings, and network segments. Ensure that the addressing scheme allows for future growth. |
|  | • | **Network Hardware and Software Requirements:** List the specific hardware (routers, switches, access points, etc.) and software (network operating systems, monitoring tools, etc.) required for the network. Include specifications and quantities. |
|  | • | **Security Design:** Outline the security measures to be implemented, including firewalls, intrusion detection/prevention systems, and encryption protocols. Define access control policies and mechanisms to protect sensitive data and resources. |
|  | • | **Wireless Network Design:** If the campus includes wireless connectivity, provide a detailed design for the wireless network. Specify the placement of access points, frequency channels, and security measures such as WPA3 encryption. |
|  | • | **Network Management and Monitoring:** Define how the network will be managed and monitored. Include details on network management tools, protocols, and procedures for monitoring network performance, troubleshooting, and reporting. |
|  | • | **Quality of Service (QoS) Design:** If applicable, design the Quality of Service policies to prioritize certain types of traffic, ensuring that critical applications receive the necessary bandwidth and resources. |
|  | • | **Documentation:** Create comprehensive documentation that includes network diagrams, device |

|  |  |
| --- | --- |
|  | configurations, IP address assignments, and any other relevant information. This documentation will be essential for maintenance, troubleshooting, and future expansion.   * **Implementation Plan:** Develop a detailed plan for implementing the network. Include a timeline, tasks, responsibilities, and any potential challenges or risks. Consider phased implementation to minimize disruptions. * **Testing and Validation:** Define a testing plan to validate the functionality and performance of the network. This may include simulated load testing, security assessments, and user acceptance testing. * **Training Plan:** Develop a plan for training IT staff, administrators, and end-users on the new network infrastructure. Include training materials and schedules. * **Maintenance and Support Plan:** Outline the procedures for ongoing maintenance and support of the network. Include details on software updates, hardware replacements, and troubleshooting processes. * **Budget and Resource Allocation:** Provide a detailed budget that includes costs for hardware, software, labor, and any other expenses. Allocate resources appropriately to ensure a successful implementation. |
| Benefits | With every advancement in information technology there is an acceleration in adoption. This makes upgrading your network services more important than ever. High-speed, reliable networks are the backbone of any successful business, and a robust network infrastructure can |

|  |  |
| --- | --- |
|  | help you stay competitive and agile. From faster data transfer speeds to enhanced security features, upgrading your business network infrastructure and services offers many benefits that can have a significant impact on your bottom line. your business. In this blog, we will explore seven benefits of upgrading network services for your business. We will also explore how they can help you stay ahead of your competitors. Improve speed and performance. If your legacy network or infrastructure is outdated or performing poorly, it can negatively impact your organization or business in many ways. For example, slow speeds can frustrate customers and employees, and unreliable connections can lead to increased costs, lost productivity, and revenue. Network upgrades can significantly improve your network speed and performance. This can lead to faster file transfers, improved application performance, and a better overall user experience. With faster speed and performance, you can upgrade your hardware, such as routers, switches, and 15 modems. You can also upgrade your software, such as your network operating system and security software. Improved reliability and availability. Unreliable or outdated networks can cause outages, potentially leading to lost productivity and revenue, and security breaches can expose sensitive data. By upgrading your network infrastructure, you can ensure your systems run smoothly and efficiently. This will reduce the risk of downtime and outages and create less disruption. A reliable network can also improve customer satisfaction by minimizing service disruptions and providing faster, more consistent access to your products and services. In today's rapidly changing business environment, a reliable network is more essential than ever, allowing you to stay competitive and meet growing customer demands. Enhanced security. Upgrading your network services is essential to keep your organization secure in this environment. Upgrading your network means benefiting from the latest and most advanced security features and compliance with industry standard protocols. Upgraded network services often come with more advanced security features, including firewalls, intrusion detection |

|  |  |
| --- | --- |
|  | and prevention systems, and encryption protocols. This provides better protection against cyber threats. A managed service provider can evaluate your current network configuration and offer appropriate upgrades to ensure all endpoints are secure. With industryleading network management services and advanced security capabilities, you can focus on growing your business instead of worrying about cyber threats. Better scalability. Scalable networks can easily be expanded or scaled down as your business needs change. This is essential for businesses experiencing rapid growth or facing traffic spikes. Upgraded networks can often accommodate and manage growing numbers of users, devices, and applications, allowing businesses to expand their operations. 16 There are a few things you can do to check if your network is scalable. First, look at your current network usage. If you regularly use up your network capacity, you may not be able to expand. Alternatively, you can talk to a network engineer or an IT and management consultant. They can help you evaluate your network's scalability and make suggestions for improvements. Improve collaboration and communication. Network upgrades can also improve collaboration and communication within your organization, which is essential for success. Upgrading your network services can significantly improve both aspects of your business. With faster internet speeds and better connections, employees can work together more effectively and efficiently. They can share files, collaborate on projects, and communicate with each other more easily. Video conferencing and other telecommunications tools are becoming more reliable, allowing for seamless communication with colleagues and customers around the world. By upgrading your network services, you are investing in the future of your business and fostering a culture of collaboration and communication. With these improvements, you can expect increased productivity, higher employee satisfaction, and ultimately better financial results. Cost savings. Upgrading your network services can significantly improve your business productivity and your wallet. Upgrading your organization's network services can save |

|  |  |
| --- | --- |
|  | money. By investing in newer, more efficient technology, you can benefit from faster Internet speeds, better connections, and improved security features. Upgraded network services can also eliminate downtime, increase workflow, and reduce resources used to troubleshoot network issues. Additionally, modern technologies require less maintenance, leading to lower long-term costs. Competitive advantage. 17 Ultimately, like all businesses, you strive for success and seek an edge to stay ahead of the competition. One way to do this is to upgrade your network services. With increasing reliance on the latest technologies and the need for quick and efficient communication, having a network that can meet the demands placed on it is a must. Investing in upgrades and tools like faster Internet speeds and secure network connections can increase productivity. Additionally, it ensures the safety and security of your sensitive information. It is imperative to stay ahead of the curve. Upgrading your network services is a smart move for any business that wants to stay competitive in today's market. Benefits of using a managed service provider Partnering with a managed service provider (MSP) to upgrade network services can benefit organizations. Managed service providers bring expertise and experience in modern infrastructure, ensuring network maintenance and upgrades are carried out smoothly and efficiently. They can provide proactive monitoring and maintenance services, identifying and resolving problems before they become major problems. Managed service providers can also provide customized solutions tailored to an organization's unique needs. This ensures that network upgrades meet specific goals and requirements. With an MSP managing network upgrades, organizations can focus on core operations and operations instead of maintaining IT infrastructure. Overall, working with MSPs to upgrade network services can improve efficiency, reduce downtime, and ensure organizations have access to the latest technologies and services. Upgrading network services will benefit your business. With faster speeds and increased bandwidth, enhanced network services provide faster and more reliable connections, enabling |

|  |  |
| --- | --- |
|  | faster data transfers and improved productivity. Advanced security measures and native services can provide additional protection against cyber threats, protect sensitive data, and minimize the risk of cyber-attacks. Additionally, upgraded network services can support the latest technologies and applications. This provides access to advanced tools, software installations and services that drive innovation and competitiveness. Ultimately, working with a managed service provider to update your network services can improve efficiency, security, and innovation. This makes it a valuable investment in your company's digital capabilities. |
| stakeholders | Researches  Newspaper readers Developers |
| Risks | Risk identification the first element of a cybersecurity risk management framework is risk identification. 58 It is the process of identifying sources, events, and situations that could harm your network, such as hackers, malware, natural disasters, human error, or device failure. You should also identify assets at risk, such as data, devices, systems or services, and their value to your organization. Risk identification helps you establish scope and context for managing your cyber security risks. Risk analysis the second element of the cybersecurity risk management framework is risk analysis. This is the process of estimating the likelihood and impact of each risk identified on your network. You can use qualitative or quantitative methods or a combination of both to assess the likelihood and severity of risks. 59 You should also review existing controls and vulnerabilities that impact your cybersecurity. Risk analysis helps you prioritize risks and determine the level of risk you are willing to accept. Risk handling the third element of the cybersecurity risk management framework is risk treatment. This is the process of selecting and implementing appropriate measures to address the risks you have analysed. There are four main strategies you can choose to address risk: avoid, reduce, transfer, or accept. Avoiding risk means eliminating the source or activity that causes the risk. 60 Risk reduction means implementing control or mitigation |

|  |  |
| --- | --- |
|  | measures to reduce the likelihood or impact of a risk. Transferring risk means transferring responsibility or costs to another party, such as an insurance company or seller. Accepting risk means recognizing and accepting it, either because it is too low or because handling it is too costly. Addressing risk helps you balance the costs and benefits of cybersecurity. Monitor and review risks the fourth element of the cybersecurity risk management framework is risk monitoring and review. This is the process of monitoring and evaluating the performance and effectiveness of your risk measures. 61 You should monitor changes in the internal and external environment that may impact your cybersecurity, such as new threats, technologies, regulations, or business goals. You should also consider the results and consequences of your risk management measures, such as incidents, audits, testing or feedback. Risk monitoring and review helps you identify gaps and opportunities for improvement in your cybersecurity risk management. Risk communication and consulting the fifth element of the cybersecurity risk management framework is risk communication and consultation. It is the process of sharing and exchanging information and opinions about cybersecurity risks and how to handle them 62 between relevant parties such as managers, employees, customers, partners, or regulatory agencies. You must communicate and consult with stakeholders throughout the risk management process, from identification to review, to ensure their awareness, engagement, and support. Risk communication and advice helps you build confidence in managing your cybersecurity risks. Risk Reporting and Documentation Risk reporting and documentation make up the sixth element of a methodology for managing network security risks. This is the process of accurately and consistently documenting and presenting facts and information relevant to network security threats and their management. The risk identification, analysis, treatment, monitoring, and review processes and outcomes must all be documented and reported, as well as the risk management policies, procedures, roles, and |

|  |  |
| --- | --- |
|  | responsibilities. To record and present the network security risks, you may use a variety of formats and tools, such as risk registers, matrices, dashboards, or reports. You may show and enhance your network security risk management with the aid of risk 63 documentation and reporting. |
| Assumptions | * **User Distribution:**    + **Assumption:** Users are evenly distributed across the campus.   + **Rationale:** This assumption simplifies initial planning, but adjustments may be needed if user density varies significantly in certain areas. * **Bandwidth Requirements:**    + **Assumption:** The assumed bandwidth requirements for different departments and user groups are based on typical usage patterns. o **Rationale:** This simplifies the initial design, but periodic assessments are needed to ensure that bandwidth requirements align with actual usage. * **Device Types and Connectivity:**    + **Assumption:** Users primarily connect using standard devices (laptops, smartphones), and the network design supports standard connectivity requirements.   + **Rationale:** While this simplifies the design process, adjustments may be necessary for specialized devices or connectivity needs. * **Traffic Patterns:**    + **Assumption:** Traffic patterns follow general trends, and there are no |

|  |  |  |
| --- | --- | --- |
|  |  | significant deviations in application usage.  o **Rationale:** This assumption allows for a baseline design but may need adjustment if certain applications or services have unique traffic patterns. |
|  | • | **Security Policies:**   * **Assumption:** Standard   security policies, including firewalls and access controls, are sufficient for the campus network.   * **Rationale:** Assuming a   baseline level of security helps create a standard framework but may require customization based on specific security needs or compliance requirements. |
|  | • | **Physical Infrastructure:**   * **Assumption:** Existing physical infrastructure, such as cabling and power supplies, meets the network requirements. * **Rationale:** This assumption simplifies the design process, but a thorough infrastructure assessment is essential to identify and address any deficiencies. |
|  | • | **Application and Service Availability:**   * **Assumption:** Critical applications and services required by the campus community are generally available and reliable. * **Rationale:** This assumption simplifies initial planning but requires ongoing monitoring to address any issues that may arise. |

|  |  |  |
| --- | --- | --- |
|  | • | **Budget Constraints:**   * **Assumption:** The project will be executed within the allocated budget, and there are no unexpected financial constraints. * **Rationale:** While budgets are subject to change, assuming a predefined budget helps in creating a realistic initial plan. |
|  | • | **Future Growth:**   * **Assumption:** The campus   will experience growth, but the rate and scale are within typical expectations.   * **Rationale:** This assumption allows for a scalable design that can accommodate expansion without significant modifications. |
|  | • | **Staff Competency:**   * **Assumption:** The IT staff responsible for network implementation and maintenance possess the necessary skills and expertise. * **Rationale:** Assuming a certain level of competency allows for planning without the need for extensive training considerations, but it's important to address any skill gaps that may exist. |
|  | • | **Collaboration and**  **Communication Tools:**   * **Assumption:** Standard collaboration and communication tools meet the needs of the campus community. * **Rationale:** This simplifies the design process but may require adjustments if |

|  |  |
| --- | --- |
|  | specific tools or integrations are needed. |
| Project team  Role in the project | Bornwise baloyi member  Roandiswa Mbezi secretary  Mamabolo mokgadi member  Solomon Moshoka leader |
| Summary budget | Budget   1. Hardware Costs:   Networking Equipment (Switches, Routers, Access Points): This will be a significant expense, and costs depend on the brand, capacity, and features of the equipment. Estimate R20,000 to R40,000.  Cabling and Infrastructure: Costs for structured cabling, fiber optics, and other network infrastructure components. Estimate R5,000 to R10,000.  Security Appliances (Firewalls, Intrusion Detection/Prevention): These are essential for network security. Estimate R5,000 to R10,000.   1. Software Costs:   Network Management and Monitoring Software:  Estimate R2,000 to R5,000 for software licenses.  Security Software (Antivirus, Anti-Malware):  Estimate R1,000 to R2,000 for licenses.  VLAN Configuration Software: Estimate R500 to R1,000.  Labor Costs:  Network Design and Implementation: Hiring network engineers or consultants for the initial setup. Labor costs can vary greatly, but estimate R20,000 to R40,000.  Ongoing Network Maintenance: Depending on your in-house IT team or external support, you may need to budget R10,000 to R20,000 annually for maintenance 4. Bandwidth Costs:  Internet Service Provider (ISP) Fees: Monthly or annual fees for the internet connection. Estimate R5,000 to R10,000 annually.  5. Miscellaneous Costs:  Training: Budget for training staff and administrators on network management and security. Estimate R2,000 to R4,000. Warranty and Support Contracts: Costs for ongoing support and equipment warranties.  Estimate R5,000 to R10,000 annually. |
|  | 6. Contingency:  It's a good practice to include a contingency fund of 10-15% of your total budget to account for unexpected expenses. 7. Total Budget Estimate:  Based on the above estimates, a rough budget for the initial setup could range from R50,000 to R100,000, with an additional R15,000 to R30,000 in annual recurring expenses for maintenance and internet connectivity.        Absolutely, here are 100 serial numbers allocated to computers, switches, routers, printers, and a server: Computers:  PC-0001  PC-0002  PC-0003 ...  PC-0097  PC-0098  PC-0099  PC-0100  Switches (4 total):  SW-0001  SW-0002  SW-0003  SW-0004  Routers (4 total):  RT-0001  RT-0002  RT-0003  RT-0004  Printers (3 total):  PR-0001  PR-0002  PR-0003  Server (1 total):  SRV-0001  These serial numbers follow a consistent pattern with a prefix indicating the device type and a unique identifier. You can adjust these as needed to suit your organization's tracking and identification needs. |
|  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Communcation plan | Product | Target | media | when | responsible |
|  | Project planning meeting Discussion | PROJECT  GROUP | IIT PREMISES | 06 JUNE 2023 | PTOJECT GROUP |
|  | Project status  meeting | PROJECT  GROUP | IIT PREMISES | O5 JULY 2023 | PROJECT GROUP |
|  | Project  document  meeting | SECRETARY | IIT PREMISES | 16 AUGUST  2023 | PROJECT GROUP |
|  | Developme  nt status meeting | PROJECT GROUP | IIT PREMISES | 20 SEPT 2023 | PROJECT  GROUP |
|  | Q\A | PROJECT GROUP | IIT PREMISES | 11 OCT 2023 | PROJECT  GROUP |

|  |  |  |
| --- | --- | --- |
| Milestone / deliverable | Target |  |
| Project start | 06 June 2023 |  |
| Project plan and review and completion | O5 JULY 2023 |  |
| Project initiation | O5 JULY 2023 |  |
| Planning completion | 16 AUGUST 2023 |  |
| Execution completion | 20 SEPT 2023 |  |
| Monitoring and control completion | 11 OCT 2023 |  |
| Project completion | 17 NOV 2023 |  |

REFERENCE LIST

# References List

Brayt, D. (2021, August 17). *Khan Academy*. Retrieved from khanacademy.org: http://www.khanacademy.org

Chen, A. (2019, February 24). *IEEE Xplore*. Retrieved from ieeexplore.ieee.org: http://www.ieeexplore.ieee.org

Jackson, D. (2020, June 18). *Encyclopedia Britannica*. Retrieved from britannica.com: http://www.britannica.com

Paker, D. (2012, May 20). *Google Scholar*. Retrieved from scholar.google.com: http://www.scholar.google.com

Smith, P. (2022, October 27). *National Archives*. Retrieved from archives.gov: http://www.archives.gov