

|  |  |
| --- | --- |
| **Project Initiation Document (PID)** | |
| **Project Title** | **IT Security and Infrastructure Enhancement** |
| **Company** | **57th Global Tyres** |
| **Prepared by** | **Owolabi Olasubomi** |

**Table of** **Contents**

[**Project Background** 3](#_Toc203116319)

[**Mission Statement** 3](#_Toc203116320)

[**Vision Statement** 3](#_Toc203116321)

[**Project Objectives** 3](#_Toc203116322)

[**Departments and Scope of Work** 4](#_Toc203116323)

[**Key Deliverables** 4](#_Toc203116324)

[**Roles and responsibilities** 5](#_Toc203116325)

[**Project Timeline** 5](#_Toc203116326)

[**Project Budget** 5](#_Toc203116327)

[**Risk Assessment** 6](#_Toc203116328)

[**Communication Plan** 6](#_Toc203116329)

[**Training & Awareness** 6](#_Toc203116330)

[**Monitoring & Review** 6](#_Toc203116331)

# **Project Background**

This project simulates the role of an IT professional at 57th Tyres Global, a fast-growing tyre sales and distribution company based in Lagos, Nigeria, that aims for global expansion. The company employs between 50 and 200 people, including on-site and remote staff.

In Lagos’ competitive market, where customer trust is vital, 57th Tyres Global has a strict zero-tolerance policy for actions that could harm its reputation. Protecting customer data, ensuring business continuity, and maintaining operational excellence are core values of the organization.

# **Mission Statement**

Our goal is to provide durable, safe, and affordable tyres while establishing a standard for excellence and innovation in the automotive industry across Africa and beyond.

# **Vision Statement**

We aim to be the most trusted tyre brand in West Africa, recognized globally for our quality, customer service, and operational integrity.

# **Project Objectives**

* Achieve ISO 27001:2022 certification by the end of the project timeline
* Protect sensitive information, including client data, proprietary training materials, and internal intellectual property
* Ensure compliance with relevant regulations, such as GDPR and NDPR
* Enhance the company’s market positions by leveraging ISO 27001:2022 certification
* Establish information security governance and increase the awareness of 57th global tyres team of information security principles

# **Departments and Scope of Work**

| **Department** | **No. of Users** | **Critical Assets** |
| --- | --- | --- |
| Legal | 5 | Laptops, Legal Document Repository, External Drive, Contract Management Software |
| Human Resources | 6 | HRMIS, Laptops, Payroll Software, Staff Database |
| IT | 8 | Servers, Network Switches, Firewalls, Admin Laptops, Monitoring Tools |
| Supply Chain | 9 | Inventory Software, Laptops, Barcode Scanners, Delivery Schedule System |
| Sales | 10 | CRM, POS Machines, Mobile Devices, Sales Dashboard |
| Facilities | 4 | CCTV Systems, Access Control Units, Maintenance Scheduling Software |
| Operations | 7 | Production System, Industrial PCs, Asset Trackers, Operations Dashboard |

# **Key Deliverables**

* Asset Inventory by Department
* Security Gap Assessment Report
* Risk Treatment Plan
* Staff Awareness Training
* Policy Documents (Acceptable Use, Access Control, Data Classification)
* Implementation of Antivirus, Firewalls, Backup Systems
* Final Project Report and Recommendations

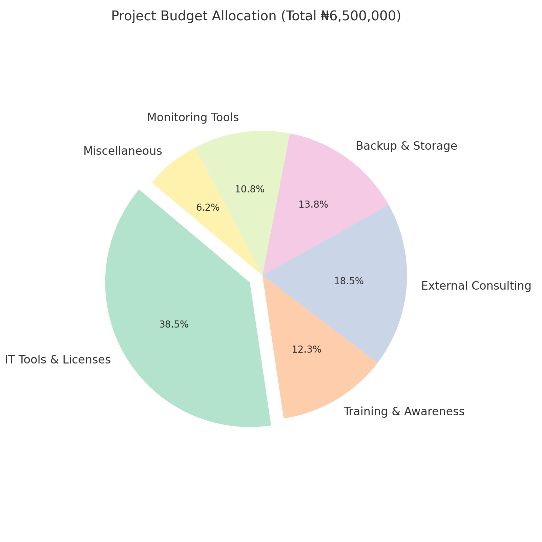
# **Roles and responsibilities**

* **Project sponsor, [pascal riwaan] CEO** – Provides strategic direction and ensure alignment with business goals
* **Project manager: [Owolabi Olasubomi] IT contractor –** oversee the project, manage resources and ensure timely delivery
* **Deaprtment heads –** Ensure department specific compliance with ISMS policies
* **Employees –** participate in trainings and adhere to isms policies

# **Project Timeline**

| **Phase** | **Duration** |
| --- | --- |
| Project Kickoff | 1 Week |
| Asset Inventory & Audit | 2 Weeks |
| Risk & Gap Assessment | 2 Weeks |
| Implementation | 4 Weeks |
| Training & Awareness | 2 Weeks |
| Monitoring Setup | 1 Week |
| Final Review & Reporting | 1 Week |

# **Project Budget**



# **Risk Assessment**

| **Risk Description** | **Likelihood** | **Impact** | **Mitigation Strategy** |
| --- | --- | --- | --- |
| Resistance to change by staff | Medium | High | Conduct awareness sessions and demos |
| Data loss during implementation | Low | High | Perform backups before changes |
| Vendor delays in tool procurement | Medium | Medium | Use multiple vendors; pre-negotiate timelines |
| Incompatibility with legacy systems | Low | Medium | Test updates in sandbox before deployment |
| Budget overrun | Medium | Medium | Track spent weekly and report variances |

# **Communication Plan**

| **Audience** | **Frequency** | **Channel** | **Responsible** |
| --- | --- | --- | --- |
| Project Team | Weekly | Email, WhatsApp | Project Lead |
| Management | Bi-weekly | Summary Reports | IT Lead |
| Department Heads | At Milestones | Progress Meetings | Project Lead |
| All Staff | Monthly | Bulletin, Email | HR/Comms |

# **Training & Awareness**

* Mandatory Cybersecurity Awareness Training for all departments
* Role-specific sessions for HR, Legal, and Sales systems
* Posters, infographics, and email campaigns for reminders
* Post-training assessments to measure understanding
* Optional video tutorials for common IT practices (MFA, backups)

# **Monitoring & Review**

* Weekly audit logs and monthly reports
* Quarterly internal IT reviews to assess progress
* A post-project review and user feedback survey to identify gaps