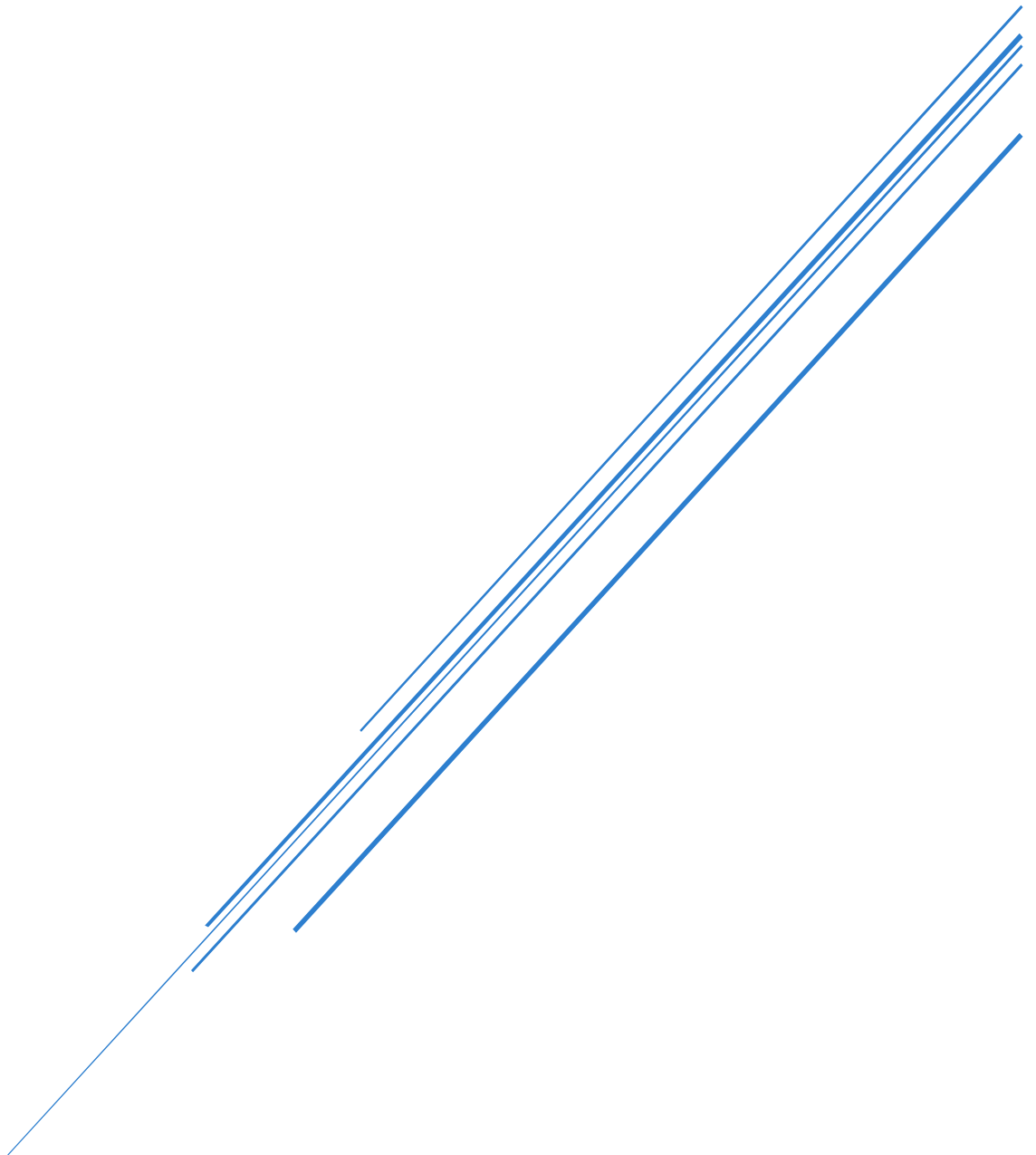


BUSINESS REQUIREMENTS DOCUMENT: HSS (HEALTHCARE STAFF SECURE)

Team: CyberTransformers



ITWeb Security Summit 2025

Table of Contents

Purpose of this Document	2
Business Requirements	2
Stakeholder Requirements	2
Business Processes	2
Scope and Limitations	2
Glossary	3
Appendix	3
Approval & Sign-off	3
Conclusion	3

1. Purpose of this Document

This document defines the business requirements for the development and implementation of the Healthcare Staff Secure (HSS) Identity and Access Management (IAM) system. It outlines the business objectives, key requirements, involved stakeholders, business processes, and scope. It serves as a foundation for approval and guides the project throughout its lifecycle.

2. Business Requirements

- Provide secure, role-based access control to healthcare systems.
- Enable multi-factor authentication for healthcare staff.
- Ensure compliance with South African POPIA and international HIPAA regulations.
- Deliver real-time security alerts, awareness tips, and threat trends via an AI chatbot.
- Detect and respond to unusual behaviour through AI-based anomaly detection.
- Offer affordable access through a Pay-As-You-Go pricing model.

3. Stakeholder Requirements

Stakeholder	Requirement
Healthcare Institutions	Scalable IAM that protects patient and staff data without upfront costs.
IT Administrators	Easy integration, detailed access logs, and customizable user roles.
Hospital Staff	Simple, secure access and timely alerts on threats.
Regulatory Authorities	Compliance reporting aligned with POPIA and HIPAA.
Investors/Partners	Commercially viable system with ROI and growth potential.

4. Business Processes

The HSS system supports the following key processes:

- **User Authentication:** Staff log in with multi-factor authentication and receive access based on predefined roles.
- **Access Management:** Admins assign, modify, and revoke access roles as needed.
- **Alert & Awareness:** AI chatbot sends real-time messages to users about login risks, phishing trends, and best practices.
- **Monitoring & Response:** System continuously tracks user behaviour to flag and react to abnormal activities.

5. Scope and Limitations

- **Scope**
 - Identity and access management for healthcare institutions.
 - Real-time AI alerts and behaviour monitoring.
 - Role-based permissions and multi-factor login.
 - Web-based interface with admin controls.

- **Limitations**

- Only available as a web platform (no mobile app yet).
- Not a full antivirus or network security tool.
- Requires internet access for full functionality.
- AI only covers security alerts, not full user support.

6. Glossary

Term	Definition
IAM	Identity and Access Management
POPIA	Protection of Personal Information Act (South Africa)
HIPAA	Health Insurance Portability and Accountability Act (USA)
MFA	Multi-Factor Authentication
AI Chatbot	Automated tool that delivers alerts and security tips to users
Behavioural Anomaly	Abnormal access activity suggesting a possible security threat

7. Appendix

- CyberInsider article: "Everest Ransomware Group Hits R5B Hospital Chain Mediclinic," May 2025

8. Approval & Sign-off

Name	Role	Signature	Date
Mahlatsi Lucky Mpilo	Business Analyst		03/06/2025
Bandile Ndlovu	Security Analyst		03/06/2025
Tshegofatso Mkhabela	Developer		03/06/2025
Vukile Ntsele	Developer		03/06.2025
Shawn Chareka	Developer		03/06/2025

9. Conclusion

HSS addresses the urgent cybersecurity needs of healthcare providers by offering a flexible, AI-enhanced IAM system. With scalable pricing and compliance-ready features, it supports South African healthcare institutions in protecting sensitive data and responding proactively to cyber threats.