2/5/2025

Comprehensive System Deployment and Lifecycle Documentation for the Research Grant Proposal Application System - University of Kabianga

First Official Draft

Knoph O. Ayieko & Felix Kiprotich

SYSTEM DEVELOPERS

Comprehensive System Deployment and Lifecycle Documentation for
The Research Grant Proposal Application System

University of Kabianga

Prepared by:
Knoph O. Ayieko (System Developer)
Felix Kiprotich (System Developer)

Submitted to:
University of Kabianga - Research Committee
UOK DVC (PRD)

Date of Submission:
11th February, 2025 - Wednesday

This is an official **System Deployment, Compliance and Lifecycle** documentation

DOCUMENT OVERVIEW AND ALTERNATIVE TITLES

Introduction to the Documentation

This document serves as the official **Comprehensive System Deployment and Lifecycle Documentation for the Research Grant Proposal Application System - University of Kabianga**. It provides a structured reference covering system deployment, compliance, governance and ongoing monitoring. The document is designed to support all stakeholders, including university administrators, researchers and IT personnel, in ensuring smooth implementation, security and long-term operational sustainability.

The primary objective of this documentation is to:

- Provide a step-by-step guide on system deployment and implementation.
- Outline post-deployment support and maintenance procedures.
- Ensure compliance with legal, regulatory and security requirements.
- Define a structured plan for ongoing monitoring, evaluation and future system upgrades.

Alternative Considerations for the Document Title

Depending on the context, this documentation may also be referred to as:

- Comprehensive System Implementation and Management Report
- End-to-End System Deployment and Governance Manual
- System Development, Deployment and Maintenance Handbook

These alternative titles highlight the document's extensive scope, from development to post-deployment governance.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

UOK / UoK	-	University of Kabianga
DVC	-	Deputy Vice Chancellor
PRD / PR&D	-	Planning, Research & Development
RGPAS	-	Research Grant Proposal Application System

CHAPTER 1: INTRODUCTION

1.1 Background of the System

The **Research Grant Proposal Application System (RGPAS)** is an innovative, fully digitalized solution developed for the **University of Kabianga (UoK) Research Committee under the Deputy Vice Chancellor - Planning, Research & Development**. This system streamlines the process of research grant proposal submissions, evaluations, approvals and funding disbursements. It is designed to replace the conventional manual application process with an efficient, transparent and accessible online platform, ensuring ease of use for researchers while maintaining high security and compliance standards.

1.2 Purpose of the Document

This document serves as a **comprehensive guide** for the deployment, implementation and lifecycle management of the **RGPAS**. The objectives of this document include:

- Providing clear **deployment guidelines** to ensure a smooth transition from development to live implementation.
- Defining **post-deployment operational strategies**, including user support, maintenance and system upgrades.
- Outlining **legal, compliance, and security considerations** to align with institutional and national IT policies.
- Establishing an **evaluation framework** for tracking system performance, user engagement and effectiveness.
- Ensuring that all **stakeholders, including IT personnel, researchers and university administrators,** have a structured reference document for system governance.

1.3 Scope of the Document

This document covers all **technical, administrative and compliance** aspects of the **Research Grant Proposal Application System** and is structured into the following key sections:

1. **Deployment and Implementation Documentation:** Covers system setup, infrastructure, user onboarding and go-live strategy.
2. **Post-Deployment Documentation:** Outlines operational procedures, system maintenance and user support.

3. **Legal and Compliance Documentation:** Includes IT policies, data protection compliance and security protocols.
4. **Project Closure Documentation:** Details project handover, documentation archiving and system review.
5. **Ongoing Monitoring and Evaluation Documentation:** Provides performance tracking, system audits and future upgrade recommendations.

1.4 System Overview

The **Research Grant Proposal Application System (RGPAS)** consists of several core modules:

- **User Management:** Enables role-based access control for researchers, reviewers and administrators.
- **Proposal Submission & Review:** Allows researchers to submit proposals and reviewers to evaluate applications.
- **Funding Approval & Disbursement:** Streamlines grant approvals and fund allocations.
- **Reporting & Analytics:** Provides real-time insights into research applications, approvals and fund usage.
- **Security & Compliance:** Ensures data protection, authentication mechanisms and adherence to institutional policies.

1.5 Key Stakeholders

The successful deployment and operation of the **RGPAS** require collaboration among various stakeholders, including:

- **University of Kabianga Research Committee:** The primary decision-makers and system beneficiaries.
- **Deputy Vice Chancellor (Research) Office:** Responsible for system oversight and administrative implementation.
- **ICT Department (University IT Team):** Ensures technical support, maintenance and cybersecurity enforcement.
- **Researchers & Academicians:** The primary users of the system, responsible for submitting grant applications.

- **System Developers (Knoph O. Ayieko & Felix Kiprotich):** Responsible for software development, deployment and continuous improvement.

1.6 Assumptions and Constraints

1.6.1 Assumptions

- The system will be **fully hosted on the university's ICT infrastructure** or a secure cloud-based solution.
- All **users (researchers, evaluators and administrators) will be trained** before system rollout.
- The **university will allocate the necessary budget** for ongoing system maintenance and upgrades.

1.6.2 Constraints

- The system must comply with **Kenya's Data Protection Act (2019)** and **institutional IT policies**.
- Network and server capacity may **impact system performance**, requiring optimized hosting solutions.
- User adoption may require an **initial learning curve**, necessitating continuous user support and training.

CHAPTER 2: SYSTEM DEPLOYMENT AND IMPLEMENTATION DOCUMENTATION

2.1 Deployment Strategy

The deployment of the **Research Grant Proposal Application System (RGPAS)** at the **University of Kabianga (UoK)** follows a structured, phased approach to ensure a smooth transition from development to full-scale operation.

The deployment strategy consists of:

1. **Pre-Deployment Preparation:** Ensuring all infrastructure, resources and configurations are in place.
2. **System Installation & Configuration:** Setting up the application on the university's hosting environment.
3. **Testing & Quality Assurance (QA):** Conducting system, security and user acceptance tests.
4. **User Training & Onboarding:** Familiarizing users with system functionalities.
5. **Pilot Rollout:** Implementing the system on a limited scale to identify and resolve any issues.
6. **Full System Deployment:** Official system launch for all users.
7. **Post-Deployment Support:** Providing ongoing technical support and system monitoring.

2.2 Pre-Deployment Activities

Before deployment, the following preparatory activities are undertaken:

2.2.1 Infrastructure Readiness

- Setting up **dedicated university servers** or cloud hosting solutions.
- Configuring **secure database storage** with backup solutions.
- Ensuring **network bandwidth and load balancing** capabilities.

2.2.2 Security and Compliance Checks

- Implementing **data encryption** for secure communication.
- Configuring **role-based access control (RBAC)** for system users.
- Ensuring compliance with **Kenya's Data Protection Act (2019)**.

2.2.3 System Configuration & Customization

- Customizing the system's **interface, workflows and user roles** based on university needs.
- Integrating **authentication mechanisms** (university login credentials, two-factor authentication).
- Setting up **notification systems** (email/SMS alerts for submissions and approvals).

2.3 System Installation and Configuration

2.3.1 Hosting & Server Deployment

Hosting Model: On-premises university servers or a cloud-based environment.

Server Requirements:

- **Operating System:** Linux-based (Ubuntu, CentOS) or Windows Server.
- **Database:** MySQL/PostgreSQL.
- **Web Server:** Apache/Nginx.
- **Application Framework:** PHP (Laravel), Python (Django) or Node.js.

2.3.2 Database Setup

- Creating **user roles and permissions** within the database.
- Setting up **audit logs** for tracking system activities.
- Enabling **regular data backup mechanisms** for redundancy.

2.4 Testing & Quality Assurance

Before full deployment, the system undergoes rigorous testing:

2.4.1 Functional Testing

- Verifying **proposal submission workflow** (from researcher to reviewer to approval).
- Testing **automated notifications** (email confirmations, deadline reminders).

2.4.2 Security Testing

- Checking for **vulnerabilities (SQL injection, XSS, CSRF attacks)**.
- Ensuring **proper access control** to sensitive information.

2.4.3 Performance Testing

- Testing **system responsiveness under load** (handling multiple submissions at once).
- Checking **database query optimization** for fast data retrieval.

2.4.4 User Acceptance Testing (UAT)

- Involving **a group of researchers, evaluators and administrators** to test usability.
- Gathering **feedback for final system refinements** before go-live.

2.5 User Training and Onboarding

To ensure successful adoption, a structured training program is implemented:

2.5.1 Training Methods

- **Workshops & Live Demos:** Hands-on training for university staff and researchers.
- **User Manuals & Video Tutorials:** Providing accessible learning resources.
- **Help Desk Support:** Establishing a dedicated ICT help desk for inquiries.

2.5.2 Training Content

- **System Navigation:** Logging in, submitting proposals, reviewing submissions.
- **Data Entry & Validation:** Ensuring correct information input.
- **Access Control & Security Protocols:** Using strong passwords and account recovery.

2.6 Pilot Deployment & Initial Rollout

2.6.1 Pilot Testing Phase

- Deploying the system to **a select group of researchers and evaluators**.
- Monitoring **early-stage user feedback** and identifying issues.
- Making **necessary system adjustments** before full rollout.

2.6.2 Full System Deployment

- Official **launch announcement** and activation of the system for all users.
- Opening **system access to the university research community**.
- Implementing **real-time monitoring and support** for early users.

2.7 Post-Deployment Support and Maintenance

2.7.1 Technical Support Plan

- Establishing a **dedicated IT support team** for troubleshooting.
- Implementing **live chat, email and phone support** channels.
- Creating a **knowledge base for self-service issue resolution**.

2.7.2 System Maintenance & Updates

- **Regular system updates** to enhance functionality.
- **Database maintenance** to ensure efficiency and prevent data corruption.
- **Security patches** to fix vulnerabilities and improve data protection.

2.8 Deployment Risks and Mitigation Strategies

Potential Risk	**Mitigation Strategy**
System downtime during deployment	Deploy in **off-peak hours** & ensure backup restoration plans.
Security vulnerabilities	Conduct **penetration testing & implement security best practices**.
User resistance to change	Provide **extensive training and continuous support**.
Performance issues	Optimize **server capacity & database indexing**.

2.9 Deployment Completion and Sign-Off

- The **University ICT team and Research Committee** will conduct a **final review**.
- A **formal approval document** will be signed by all stakeholders.
- The **system will be considered officially deployed** and the next phase will focus on **post-deployment monitoring**.

2.10 Conclusion

This chapter outlined the **structured approach for deploying the Research Grant Proposal Application System (RGPAS)** at the **University of Kabianga**. With a focus on **technical readiness, user training, testing and risk mitigation**, this plan ensures **a seamless transition from development to full-scale implementation**.

CHAPTER 3: POST-DEPLOYMENT DOCUMENTATION

3.1 Overview

The deployment of the **Research Grant Proposal Application System (RGPAS)** marks the beginning of its operational phase. To ensure its long-term success, a structured **post-deployment and system management plan** is crucial. This chapter outlines the necessary steps to **monitor, maintain and improve the system**, ensuring **reliability, security and user satisfaction**.

3.2 System Monitoring and Performance Management

3.2.1 Real-Time System Monitoring

To ensure smooth operation, **real-time monitoring** is implemented for:

- **System uptime and availability**: Ensuring the system remains operational 24/7.
- **User activity logs:** Tracking logins, submissions and approvals.
- **Database health:** Monitoring queries, storage, and indexing for optimal performance.
- **Security alerts**: Detecting unauthorized access attempts or data breaches.

3.2.2 Performance Optimization

- **Regular database optimization** to prevent slow queries.
- **Load balancing & caching** to handle peak usage times.
- **Server resource scaling** for improved performance.

3.3 Technical Support and Issue Resolution

3.3.1 Support Desk and Help Center

A **dedicated IT helpdesk** will be established to handle user issues. Support services include:

- **Email and ticketing system** for structured issue tracking.
- **Live chat supports** for real-time user assistance.
- **FAQs and troubleshooting guides** for self-service solutions.

3.3.2 Bug Fixing and Software Patching

- **Regular patch updates** to fix any system bugs or security vulnerabilities.
- **User feedback-based improvements** to enhance user experience.
- **Incident response planning** to address critical failures efficiently.

3.4 Security and Compliance Management

3.4.1 User Access Control and Authentication

- **Role-based access control (RBAC)** to restrict sensitive data access.
- **Multi-factor authentication (MFA)** for added security.
- **Regular user access audits** to ensure only authorized personnel can modify data.

3.4.2 Data Backup and Disaster Recovery Plan

- **Automated daily and weekly backups** stored securely.
- **Disaster recovery protocols** to restore operations in case of failure.
- **Redundant data storage** for quick data recovery.

3.4.3 Compliance with Data Protection Laws

- **Adherence to Kenya's Data Protection Act (2019)**.
- **Data encryption and anonymization** to protect user privacy.
- **User consent management** for collecting and processing research data.

3.5 User Training and System Updates

3.5.1 Continuous User Training

- **Quarterly refresher training** for system users and administrators.
- **Updated user manuals and video guides** as features evolve.
- **Knowledge-sharing forums** for researchers and administrators.

3.5.2 System Updates and Feature Enhancements

- **New feature rollouts** based on feedback from researchers and the Research Committee.
- **Security and functionality updates** scheduled quarterly.
- **Beta testing** for new updates before full implementation.

3.6 User Feedback and System Improvements

3.6.1 Feedback Collection Mechanisms

- **Surveys and feedback forms** integrated within the system.
- **Regular user engagement meetings** to discuss system enhancements.
- **Open feedback channels** via email, forums and research forums.

3.6.2 Iterative System Enhancements

- **Prioritizing feature requests** based on user needs.

- **Fixing usability pain points** to improve efficiency.
- **Enhancing system scalability** for future institutional needs.

3.7 Risk Management and Contingency Planning

3.7.1 Identifying Potential Risks

- **Server failures** leading to downtime.
- **Data breaches or security threats** compromising research confidentiality.
- **User adoption resistance** impacting system usage.

3.7.2 Mitigation Strategies

- **Cloud-based failover systems** to ensure system continuity.
- **Regular security audits** to identify and fix vulnerabilities.
- **Comprehensive training programs** to increase user adoption.

3.8 System Audit and Compliance Reviews

3.8.1 Regular System Audits

- **Quarterly performance and security audits** conducted by the IT department.
- **Data integrity checks** to ensure correctness of research proposal submissions.
- **Compliance reviews** against university ICT policies and national regulations.

3.8.2 Governance and Reporting

- **Annual system reports** for the University of Kabianga Research Committee.
- **Audit logs and documentation** for regulatory compliance.
- **Public transparency reports** where applicable.

3.9 Long-Term System Sustainability Plan

3.9.1 Institutionalizing System Ownership

- **Dedicated ICT and Research Department oversight** to ensure system longevity.
- **Budget allocation for system maintenance and future upgrades.**
- **Partnerships with tech providers** for ongoing technical support.

3.9.2 Expanding System Capabilities

- **Integration with external research funding bodies** for broader accessibility.
- **AI-driven analytics and insights** for enhanced research data analysis.

- **Multi-institutional collaborations** for knowledge sharing and system improvement.

3.10 Conclusion

This chapter outlined the **post-deployment strategies** to ensure the smooth operation, security and sustainability of the Research Grant Proposal Application System (RGPAS). A strong **monitoring, maintenance, user support, security and compliance framework** ensures that the system continues to serve the University of Kabianga effectively.

CHAPTER 4: LEGAL AND COMPLIANCE DOCUMENTATION

4.1 Overview

Legal and compliance documentation is essential for ensuring that the **Research Grant Proposal Application System (RGPAS)** adheres to the **laws, regulations, and institutional policies** governing digital systems, data protection and research grant administration. This chapter details the legal framework, compliance measures and risk mitigation strategies for ensuring the system operates within the **University of Kabianga's ICT policies and Kenya's legal framework.**

4.2 Key Legal Frameworks and Compliance Standards

The system is required to comply with the following **legal and institutional regulations:**

4.2.1 The Kenya Data Protection Act (2019)

- **User Data Protection:** Ensures that personal and research data collected through the system is **secure, confidential and processed lawfully.**
- **Informed Consent:** Researchers and users must be informed about data collection, processing and storage policies.
- **Right to Access & Deletion:** Users must have access to their data and the right to request its deletion.
- **Data Storage and Transfers:** All research data should be stored securely within servers compliant with **Kenyan laws on data sovereignty.**

4.2.2 The Computer Misuse and Cybercrimes Act (2018)

- **Cybersecurity Requirements:** The system must implement security protocols to prevent unauthorized access, hacking, or cyber threats.
- **Protection Against Fraud:** The system must have safeguards to prevent research grant application fraud or misrepresentation.

4.2.3 Institutional Research Policies & Ethical Guidelines

- **University of Kabianga Research Ethics Guidelines:** Ensures that the research grant application process adheres to the university's ethical standards.
- **Intellectual Property (IP) Protection:** The system must ensure that submitted research proposals are **protected from plagiarism and unauthorized distribution.**

4.3 System Terms of Use & Privacy Policy

The **Terms of Use and Privacy Policy** define the **rights, obligations and legal responsibilities** of system users, administrators and stakeholders.

4.3.1 System Terms of Use

- **User Responsibilities:** Users must provide accurate information and use the system ethically.
- **Prohibited Activities:** Misuse, hacking, unauthorized access or tampering with the system is strictly forbidden.
- **Intellectual Property Protection:** Researchers **retain full rights** to their submissions, with system administrators ensuring confidentiality.
- **Liability and Indemnity:** The University is not liable for external security breaches but ensures reasonable measures to protect user data.

4.3.2 Privacy Policy

- **Data Collection & Usage:** The system collects research proposals, applicant details and submission history.
- **Confidentiality Measures:** All collected data is encrypted and stored securely.
- **Third-Party Access Restrictions:** User data is **not shared with third parties** unless legally required.

4.4 Compliance with Institutional ICT Policies

The system aligns with **University of Kabianga ICT policies,** including:

4.4.1 System Security and Access Control

- Role-based access control (RBAC) restricts user privileges.
- Encrypted authentication mechanisms, including **multi-factor authentication (MFA).**
- Regular **security audits** and penetration testing to identify vulnerabilities.

4.4.2 System Data Retention and Archiving

- **Active Research Data:** Retained for ongoing project tracking.
- **Archived Proposals:** Retained for **5+ years** before deletion, per university policy.
- **Automated Data Purging:** Deletion of redundant or outdated data for system efficiency.

4.5 Legal Agreements and User Consent

4.5.1 Researcher Agreement & Submission Policy

Before submission, all users must **digitally sign an agreement** confirming:

- The originality and authenticity of their research grant proposal.
- That they comply with ethical research and intellectual property laws.
- That they agree to the University's data retention and privacy policies.

4.5.2 Non-Disclosure Agreements (NDAs) for System Administrators

All system administrators **must sign NDAs** to protect sensitive user data and **prevent leaks or unauthorized disclosures.**

4.6 Risk Management and Compliance Monitoring

4.6.1 Identified Risks & Legal Implications

- **Data Breach Risks:** Unauthorized access or leaks leading to data privacy violations.
- **System Downtime Risks:** Failure to maintain uptime could affect research funding applications.
- **Misuse & Fraudulent Applications:** Potential for falsified data or unethical submissions.

4.6.2 Compliance Monitoring & Audits

- **Quarterly compliance audits** to ensure adherence to laws and policies.
- **University of Kabianga's ICT Department** to oversee legal compliance efforts.
- **User complaint and redress mechanisms** to handle any legal disputes.

4.7 Dispute Resolution & Legal Recourse

In the event of legal disputes related to the system, the following procedures apply:

- **Internal Resolution:** Complaints are first handled by the University's ICT & Research Committee.
- **Mediation:** If unresolved, parties engage in arbitration with university-appointed mediators.
- **Legal Action:** As a last resort, cases can be escalated to **Kenyan courts of law** under the **Kenya Data Protection Act** or **Cybercrimes Act.**

4.8 Conclusion

Legal and compliance documentation ensures that the **Research Grant Proposal Application System (RGPAS)** aligns with **Kenyan laws, cybersecurity regulations and institutional policies.** By adhering to **data protection, ethical research and ICT security guidelines,** the system maintains **transparency, security and regulatory compliance.**

CHAPTER 5: PROJECT CLOSURE DOCUMENTATION

5.1 Overview

Project closure marks the final phase of the **Research Grant Proposal Application System (RGPAS)** development. This chapter documents the **final acceptance, knowledge transfer, system handover and overall evaluation** of the project. The closure process ensures that all deliverables are met, all stakeholders are satisfied, and that the system is fully transitioned to the University of Kabianga.

5.2 Objectives of Project Closure

The primary objectives of project closure include:

- **Confirming project deliverables** meet the agreed-upon requirements.
- **Ensuring full acceptance and handover** of the system.
- **Providing final training and documentation** for system users and administrators.
- **Evaluating project success** and identifying lessons learned for future projects.
- **Archiving project documentation** for institutional reference.

5.3 System Handover and Acceptance

5.3.1 Final System Review

Before system acceptance, the University of Kabianga's Research Committee and ICT Department must **review the system's final version** to ensure:

- **All core features and functionalities** are implemented.
- **Security measures** are in place and verified.
- **System documentation** is complete and accessible.
- **User acceptance testing (UAT)** has been completed successfully.

5.3.2 System Acceptance and Sign-Off

Upon approval, the **Research Committee and ICT Department** will sign the official **System Acceptance Document**, which confirms:

- The system **meets all agreed-upon requirements** from the initial proposal.
- There are **no outstanding critical issues** affecting functionality or security.
- The University is satisfied with the **final deliverable and is ready to deploy.**

5.4 Final Training and Knowledge Transfer

To ensure successful adoption, **final training sessions** will be conducted for:

5.4.1 System Users (Researchers & Applicants)

- How to register, submit and track applications.
- Understanding automated notifications and status updates.
- Best practices for ensuring accurate data submission.

5.4.2 System Administrators (ICT Staff & Research Committee Chairperson)

- Managing user accounts and permissions.
- Monitoring submissions, approving applications and generating reports.
- Performing system updates, backups and troubleshooting.

5.4.3 Training Materials and Manuals

- User guides and video tutorials **provided for easy reference.**
- Technical documentation **shared with ICT staff for long-term maintenance.**

5.5 Performance Evaluation and Lessons Learned

5.5.1 Key Performance Indicators (KPIs)

To measure project success, the following **KPIs** will be evaluated:

- **System functionality**: Are all required features working as intended?
- **User adoption rate**: How many researchers successfully use the system?
- **Processing efficiency**: Has the grant application process improved?
- **Security compliance**: Have all cybersecurity measures been implemented?

5.5.2 Challenges Faced & Lessons Learned

A final project review meeting will document:

- Major challenges faced **during development and deployment.**
- How these challenges were addressed **and potential improvements?**
- Recommendations for future university ICT projects.

5.6 Documentation Archival and System Maintenance Plan

5.6.1 Archival of Project Documents

All project-related documents, including:

- Requirement specifications

- System design and architecture
- Testing reports and security audits
- Deployment and user manuals

These will be stored in **both digital and physical formats** for future reference.

5.6.2 System Maintenance and Support Plan

- Regular software updates **and security patches.**
- Ongoing user support **for researchers and administrators.**
- Annual system audit **to ensure continued compliance and efficiency.**

5.7 Formal Project Closure and Sign-Off

Once all project closure activities are completed, the final **Project Closure Report** will be prepared and signed by:

- **Lead Developers (Knoph O. Ayieko & Felix Kiprotich)**
- **University ICT Director**
- **DVC - Research Committee Representative**

This document formally acknowledges that the **Research Grant Proposal Application System (RGPAS)** project is complete and **officially handed over** to the University of Kabianga.

5.8 Conclusion

The successful closure of the **RGPAS project** ensures that the University of Kabianga now has a **fully operational, secure, and efficient system** for managing research grant proposals. With proper training, documentation, and ongoing support, the system is expected to enhance research administration and funding processes at the university.

CHAPTER 6: ONGOING MONITORING AND EVALUATION DOCUMENTATION

6.1 Overview

Ongoing monitoring and evaluation (M&E) ensures the **Research Grant Proposal Application System (RGPAS)** remains efficient, secure and aligned with the University of Kabianga's evolving needs. This chapter outlines strategies for **system performance monitoring, user feedback collection, security audits and continuous improvements.**

6.2 Objectives of Monitoring and Evaluation

The key objectives include:

- Ensuring **system reliability and uptime** through real-time monitoring.
- Collecting **user feedback** to improve usability and functionality.
- Conducting **regular security audits** to safeguard research data.
- Ensuring **system compliance** with ICT policies and data protection laws.
- Establishing a framework for **continuous system improvement and upgrades.**

6.3 System Performance Monitoring

A **dedicated system monitoring framework** will track the following:

6.3.1 Performance Metrics

- **System uptime and availability** (target: 99.9%)
- **Average page load speed** (target: ≤ 2 seconds)
- **Number of concurrent users** supported
- **Database performance and query response times**

6.3.2 Automated Alerts & Incident Management

- **Real-time alerts** for system failures or downtimes.
- **Incident response team** to address urgent issues.
- **Monthly performance reports** for ICT management.

6.4 User Feedback and System Enhancements

Continuous user feedback is essential for improving **usability and efficiency.**

6.4.1 User Feedback Collection Methods

- **Online surveys** for researchers and administrators.

- **Feedback forms integrated** into the system dashboard.
- **Quarterly user engagement sessions** with the Research Committee.

6.4.2 System Enhancement Process

- **Analysis of feedback** to identify areas for improvement.
- **Prioritization of feature requests** based on urgency and feasibility.
- **Scheduled updates and improvements** through quarterly releases.

6.5 Security Audits and Compliance Checks

To **protect sensitive research data**, regular security audits will be conducted.

6.5.1 Security Measures

- **Data encryption** for all stored and transmitted information.
- **User access controls and role-based authentication.**
- **Regular penetration testing** to identify vulnerabilities.

6.5.2 Compliance with Data Protection Laws

- Ensuring compliance with the **Kenya Data Protection Act (2019).**
- Adhering to **institutional ICT security policies.**
- Annual **external security audits** by third-party experts.

6.6 System Maintenance and Upgrade Plan

A **long-term maintenance plan** will be followed to keep the system up to date.

6.6.1 Routine Maintenance Tasks

- **Database optimization** and backup scheduling.
- **Bug fixes and security patches** to address vulnerabilities.
- **Performance testing** after each major system update.

6.6.2 Long-Term Upgrade Strategy

- **Scalability assessment** to handle growing user demands.
- **Feature expansions** based on user requirements.
- **Integration with other university systems** (e.g., finance, HR, research portals).

6.7 Reporting and Continuous Improvement

To ensure transparency, reports will be **generated periodically** for review.

6.7.1 Key Reporting Documents

- **Monthly performance and security reports.**
- **Quarterly user experience reports.**
- **Annual system impact assessment report.**

6.7.2 Continuous Improvement Framework

- **Annual system review** to evaluate performance against university needs.
- **Implementation of emerging technologies** (e.g., AI for automated application processing).
- **Periodic re-evaluation of policies** to align with national and global research trends.

6.8 Conclusion

Ongoing monitoring and evaluation will ensure that **RGPAS** remains secure, efficient and valuable to the University of Kabianga's research community. By continuously assessing system performance, gathering user feedback and implementing enhancements, the system will evolve to meet institutional and regulatory requirements effectively.

REFERENCES

1. **Kenya Data Protection Act (2019) -** Regulations on personal data protection and compliance.
2. **ISO 27001:2013 -** Information security management standard.
3. **University of Kabianga ICT Policy -** Institutional guidelines for system implementation and governance.
4. **Agile Development Methodology -** Best practices in iterative software development.
5. **System Documentation Best Practices -** Guidelines on structured technical documentation.

ADDITIONAL RESOURCES

1. **GitHub Repository** (Private/Internal use for version control and collaboration).
2. **Online Training Platform**
3. **Open Source Libraries and APIs** (Authentication, PDF generation, data visualization tools).

APPENDICES

Appendix A: System Itself

Screenshots & User Interface Overview

- Login & Dashboard Screens
- Research Proposal Submission Workflow

System Requirements Specification (SRS)

- Functional requirements (User roles, authentication, proposal submission, review process, notifications)
- Non-functional requirements (Performance, security, availability, maintainability)
- Technical stack (Programming languages, frameworks, database, hosting, integrations)

System Architecture and Design

- System architecture diagram (Logical and physical views)
- Database schema and entity relationship diagram
- API endpoints and data flow diagrams

System Testing and Quality Assurance Reports

- Test case scenarios and results
- Bug tracking and resolution log
- System performance and stress testing results

Appendix B: Additional Documentation

User Manuals and Training Materials

- Step-by-step user guide for researchers, reviewers, and administrators
- Video tutorials and FAQs
- System troubleshooting guide

Deployment and Maintenance Guidelines

- Server setup and configurations
- Backup and disaster recovery plan
- Security policies (Data protection, user access control, audit logs)

Legal and Compliance Documentation

- Data Protection Impact Assessment (DPIA)
- Compliance with Kenya Data Protection Act, 2019

- Institutional ICT security policies and agreements

Project Budget and Financial Overview

- Breakdown of system development costs
- Hosting and infrastructure expenses
- Projected maintenance and support costs

User Feedback and System Evaluation Reports

- Post-deployment feedback from users
- System performance evaluation metrics
- Future improvements and upgrade roadmap

Appendix C: Glossary of Terms

Definitions of Key Terms Used in the Documentation

Appendix D: Contact Information

Key Contacts for System Support & Maintenance