IT Systems Compliance Audit Report

Date: _____

Auditor: _____

Department/Area: _____

Period Covered: _____

1. Executive Summary

This audit assesses the IT systems compliance for policies, standards, procedures, and applicable regulations. The scope included network infrastructure, endpoint security, access controls, data backups, and incident response processes.

2. Objectives

- Evaluate compliance with internal IT policies and industry standards
- Identify gaps or risks in systems and operations
- Provide recommendations for corrective actions

3. Scope

- Systems Reviewed: [List Main Systems]
- Facilities: [List Locations, if applicable]
- Timeframe: [Start Date] to [End Date]

4. Findings

#	Area	Description	Risk Level	Recommendation	Responsible
1	Access Control	Inactive user accounts not reviewed periodically.	Medium	Implement quarterly user access reviews.	IT Manager
2	Data Backup	Backups are not tested for restorability.	High	Conduct regular backup restore tests.	IT Support
3	Patch Management	Delayed application of critical security patches on servers.	High	Establish and enforce patch management schedule.	IT Administrator

5. Recommendations

- Enforce regular access and permission reviews.
- Test backup and restore procedures every quarter.
- Apply security patches as per policy timelines.
- Update incident response plans and conduct training.

6. Conclusion

The audit identified several areas for improvement in IT systems compliance. Management should address the findings to reduce risk and maintain regulatory alignment.

Auditor Signature: _____

Date: _____