IT Systems Internal Control Checklist

Document Details

Department	IT	**Date**	_____
Prepared By	_____	**Reviewed By**	_____
System Name	_____		

Checklist

Control Area	Checklist Item	Status (Yes/No/NA)	Comments
Access Controls	Are user accounts reviewed regularly?		
	Is multi-factor authentication enabled where possible?		
	Are permissions granted based on least privilege principle?		
Data Security	Is data encrypted in transit and at rest?		
	Are regular data backups performed and tested?		
	Are data retention policies defined and followed?		
Change Management	Are changes to systems documented and approved?		
	Are changes tested before deployment?		
	Is there a rollback procedure for failed changes?		
Incident Response	Is an incident response plan in place and updated?		
	Are incidents logged and reviewed regularly?		
	Are incident response drills conducted periodically?		
Physical Security	Is access to sensitive equipment restricted and logged?		
	Are server rooms monitored for unauthorized entry?		

Important Notes

- This checklist should be reviewed and updated regularly to reflect changes in the IT environment and emerging risks.
- All responses and comments should be documented and supporting evidence retained for audit purposes.
- This document is a guide; it should be tailored to fit the organization's specific systems and risk profile.
- Completion of this checklist does not guarantee compliance but supports the assessment of internal controls.