Compliance Assessment Findings Matrix

NO.	CONTROL/REQUIREMENT	FINDING/OBSERVATION	RISK LEVEL	RECOMMENDATION	RESPONSIBLE PARTY	TARGET DATE	STATUS
1	Access Control	User accounts remain active after employee termination.	High	Implement immediate account deactivation process upon employee departure.	HR / IT	2024-07-15	Open
2	Data Encryption	Some sensitive files are stored unencrypted on local drives.	Medium	Mandate and enforce encryption for all sensitive data at rest.	IT Security	2024-08-01	Open
3	Incident Response	Incident response plan reviewed annually, not semi-annually per policy.	Low	Update review schedule and documentation to align with policy.	Compliance Team	2024-06-30	In Progress
4	Physical Security	Server room access logs not regularly reviewed.	Medium	Perform and document monthly reviews of access log data.	Facilities	2024-07-10	Open

Important Notes

- This document summarizes key compliance findings and recommended actions.
- Status updates should be regularly provided by responsible parties.
- Matrix supports monitoring and closing compliance gaps efficiently.
- Risk levels help prioritize mitigation actions according to their urgency.
- Maintain clear documentation for audit and regulatory requirements.