NIST Control ID	Required Policy	Policy Status
IA-2, IA-2(1)	Authentication and Multi-Factor Authentication Policy	**Missing**
AC-1, AC-2	Access Control Policy	**Missing**
PL-1, PL-2	Information Security Policy	**Weak**
IR-1, IR-4, IR-8	Incident Response Policy and Plan	**Missing**
AU-1, AU-2, AU-6	Logging and Monitoring Policy	**Missing**
SC-12, SC-13, SC-28	Data Protection and Encryption Policy	**Missing**
SI-12, MP-3, MP-6	Data Classification and Handling Policy	**Missing**
SR-1, SR-2, SR-3	Third-Party Risk Management Policy	**Missing**
RA-1, RA-3	Cyber Risk Assessment Policy	**Missing**
RA-5, SI-2	Vulnerability Management Policy	**Missing**
CM-1, CM-3	Change Management Policy	**Missing**
MP-1, MP-6	Removable Media and USB Policy	**Missing**
AT-1, AT-2, AT-3	Security Awareness and Training Policy	**Partial**
AC-17	Remote Access Policy	**Missing**
CM-2, CM-6	System Configuration and Hardening Policy	**Partial**
PE-1, PE-2, PE-3, PE-6	Physical Security Policy	**Implemented**
CP-1, CP-2, CP-9	Business Continuity and Disaster Recovery Policy	**Implemented**

Priority	Policy Scope / Key Requirements	Target Timeline
Critical	Define authentication requirements, MFA implementation, password standards	Month 1
Critical	Define access control principles, RBAC model, access request/approval process	Month 1
Critical	Comprehensive information security policy covering all security domains	Month 1-2
Critical	Define IR procedures, roles, escalation, notification, containment, eradication	Month 2
Critical	Define logging requirements, retention, review procedures, SIEM requirements	Month 2
High	Define encryption requirements, key management, data at rest/in transit protection	Month 2
High	Define data classification scheme, handling requirements, disposal procedures	Month 2-3
High	Define vendor assessment process, security requirements, contract clauses	Month 3
High	Define risk assessment methodology, frequency, documentation, treatment	Month 2
High	Define scanning frequency, remediation SLAs, patch management procedures	Month 2
Medium	Define change approval process, testing requirements, documentation	Month 3
Medium	Define USB restrictions, removable media controls, data transfer procedures	Month 3
Medium	Enhance existing training with role-based training, frequency, phishing simulations	Month 2
Medium	Define VPN requirements, MFA for remote access, contractor access controls	Month 2
Medium	Extend SOE baselines to all systems, define hardening standards	Month 3-4
N/A	Physical security policy exists and is well-enforced	Ongoing
N/A	BC/DR policy exists, plans tested regularly	Ongoing

Policy Owner
CISO / IT Manager
CISO / IT Manager
CISO / IT Manager
CISO / IT Manager
CISO / IT Manager
CISO / IT Manager
CISO / Data Protection Officer
CISO / Procurement Manager
CISO / Risk Manager
CISO / IT Manager
IT Manager
CISO / IT Manager
CISO / HR Manager
IT Manager / Network Team
IT Manager
Security Manager
IT Manager