

Cyber Security Back to Basics: 7 CORE CONTROLS



Data Management & Recovery:

Frequent backups, off-network.



Account Management & Access:

Strong password policy; Virtual Private Network (VPN) AND Multi-Factor Authentication (MFA) for access.



Vulnerability Management:

Security updates applied within 30 days from notification; Scan technology ecosystem monthly.



Cyber Hygiene & Awareness

Training: Continually train and test on recognizing current cyber security threats; Annual leadership briefing on security; Join a recognized cyber organization (MS-ISAC, CIS, NJCCIC).



Policies, Procedures & Incident Response:

Implement a cyber security incident response plan; Establish banking controls for wire/ACH payments.



Asset Management:

Inventory technology ecosystem including all hardware and software.



Data Management &

Protection: Define data sensitivity, owner, retention and disposal; Follow applicable laws/regulations (ie: HIPPA, NJ Reporting); Password protect/encrypt confidential data.



CYBER JIF

NJ CYBER RISK MANAGEMENT FUND

cyberjif.org