NIST CYBERSECURITY FRAMEWORK 2.0

Program Guidance

Step-by-step program to accelerate all organizations cybersecurity risk management strategy

Define Your Organizational Profile

- Define Your Current Cybersecurity Maturity Profile
- Identify Your Target Profile
- Identify critical business processes and assets
- Identify Threats, Vulnerabilities and Risks

Create Organization Security Plan – WISP Plan

- Create a Gap Analysis
- Create Action Plan

Scope Organizational Profile

- End User IT Systems
- HR IT Systems
- Third Party IT Systems
- Systems Using A/I

Protect Systems across 5 Domains

- Manage Access both Externally and Internally
- Train Users
- Monitor your network continuously
- Encrypt sensitive stored data
- Protect

Detect System Anomalies

- a. Detect Anomalies & Implications in a Timely Manner (DE.AE)
- b. Security Monitoring of Systems and Assets to identify Cyber Events (DE.CM)

Response Capability

- Build an Incident Response Plan (IRP)
- Ensure timely response during and after an Incident
- Implement protections to prevent incident expansion
- Incorporate Lessons into response plans

Recover Assets and Operations

- Build an Organizational Backup and Recovery Strategy
- Define RPO (Recovery Point Objective) and RTO (Recovery Time Objective)
- Define Roles and Responsibilities
- Execute an Annual Backup and Recovery Test

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

1-877-IT-SERVE
www.datalinknetworks.net

datalinknetworks