datalinknetworks

28110 Avenue Stanford, Unit A
Santa Clarita, CA 91355
Phone: 1-877-IT-SERVE (1-877-487-3783)
www.DatalinkNetworks.net

Datalink Networks Inc.
CYBER SECURITY CHECKLIST

□ **1. CORPORATE SECURITY POLICY**
Develop a comprehensive security policy and data governance plan that outlines school policies regarding data security and individual privacy protection.

□ **2. PHYSICAL SECURITY**
Computing resources such as servers and data stored with sensitive information need to be physical secured.

□ **3. PERSONNEL SECURITY AND USER TRAINING**
Create an Acceptable Use Policy that outlines what is appropriate use of Internet, Intranet and Extranet systems. Incorporate security policies with job descriptions and employee responsibilities that ensure compliance with associated policies. Train users not to open up attachments from untrusted sources.

□ **4. NETWORKING MAPPING**
Keep up to date network mapping of security and network infrastructure and associated connections. This mapping should outline dependencies between applications, data, and network layers to highlight any vulnerabilities.

□ **5. INVENTORY OF ASSETS**
Retain and update an inventory of both authorized and unauthorized devices accessing your network to ensure security compliance.

□ **6. ARCHITECT A LAYERED DEFENSE**
A Firewall is not adequate in today's Cyber landscape. Build a security infrastructure that incorporates Network Access Control, Server and Endpoint Protection, Intrusion Protection, Content Filtering, email filtering, SSO Controls, Data Loss Prevention and Security Monitoring Systems and Backup and Data Recovery Systems.

□ **7. AUTHENTICATION**
Consider Single Sign ON (SSO) for not only on-premise applications, but cloud applications. Utilize Multi-Factor Authentication for corporate IT Administrators and personnel with access to sensitive data.

8. INSTALL NETWORK AND SECURITY MONITORING SYSTEMS

□ Install Network Monitoring Systems that will alert you to suspicious activity from insiders and identify primary IT assets that are malfunctioning. Over half of corporate security breaches originate from insiders.

9. IMPLEMENT PATCH MANAGEMENT SYSTEMS AND SCHEDULE

□ Implement both server and client patching on a regular basis. Client machine patching can be updates and data-center assets should be updated on a regular schedule.

10. MOBILE DEVICE MANAGEMENT SYSTEM

□ Implement MDM that allows for encryption and remote device wipe, to prevent stolen devices from exposing sensitive information.

11. E-MAIL ENCRYTPTION / DLP

□ Provide email encryption when sending out sensitive corporate information, such as personnel records or SSN's.

12. AUDIT YOUR NETWORK REGULARLY

□ Conduct regular audits around network security and compliance. Make sure that your company meets SOX, and PCI compliance.