--------------------------------------------------------------------------

CYBERSECURITY AUDIT CHECKLIST

--------------------------------------------------------------------------

ORGANIZATION: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ DATE: \_\_\_\_\_\_\_\_\_\_\_\_

AUDITOR: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ DEPARTMENT: \_\_\_\_\_\_\_\_\_\_\_\_\_

--------------------------------------------------------------------------

[ ] I. GOVERNANCE AND POLICY

--------------------------------------------------------------------------

 [ ] A. Documented cybersecurity policy present

 [ ] B. Policy aligns with industry standards and best practices

 [ ] C. Regular cybersecurity awareness training for employees

 [ ] D. Incident response plan established

 [ ] E. Regular policy reviews and updates

--------------------------------------------------------------------------

[ ] II. PHYSICAL SECURITY

--------------------------------------------------------------------------

 [ ] A. Access control systems in place

 [ ] B. Surveillance systems in operation

 [ ] C. Documented procedures for handling sensitive information

 [ ] D. Secure disposal protocols for sensitive documents

 [ ] E. Equipment inventory and tracking mechanism

--------------------------------------------------------------------------

[ ] III. NETWORK SECURITY

--------------------------------------------------------------------------

 [ ] A. Firewalls implemented and regularly updated

 [ ] B. Intrusion detection/prevention systems in use

 [ ] C. Secure configuration for all network devices

 [ ] D. Regular network vulnerability assessments

 [ ] E. Wireless network secured and encrypted

--------------------------------------------------------------------------

[ ] IV. SYSTEMS AND DATA SECURITY

--------------------------------------------------------------------------

 [ ] A. Regular system and data backups

 [ ] B. Data encryption at rest and in transit

 [ ] C. Regular updates and patches for all systems

 [ ] D. Antivirus and anti-malware solutions in place

 [ ] E. Data loss prevention strategies implemented

--------------------------------------------------------------------------

[ ] V. ACCESS CONTROL

--------------------------------------------------------------------------

 [ ] A. Strong password policies enforced

 [ ] B. Two-factor or multi-factor authentication in place

 [ ] C. Least privilege access policies enforced

 [ ] D. Regular audits of user access and privileges

 [ ] E. Account lockout policies for repeated login failures

--------------------------------------------------------------------------

[ ] VI. THIRD-PARTY SECURITY

--------------------------------------------------------------------------

 [ ] A. Vendor security policies reviewed and approved

 [ ] B. Third-party data access is controlled and audited

 [ ] C. Contracts include necessary security clauses

 [ ] D. Regular security audits of third-party vendors

 [ ] E. Incident response plan includes third-party breaches

--------------------------------------------------------------------------

AUDITOR NOTES:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

------------------------------------------------------------------------------------------------------------------------