

CYBER SECURITY PROGRAM AUDIT CHECKLIST (Version 1.1)

Notes:

Primatech grants a non-exclusive license at no cost to companies who wish to use this checklist to assist in assessing their own internal cyber security programs. The use of this checklist for other purposes is prohibited.

Primatech makes no warranties, express or implied, for this checklist and accepts no liabilities for its use.

This checklist has been organized according to a variety of categories. For consistency, and more easily understood results, questions are phrased so that all "No" answers are exceptions.

The checklist addresses vulnerabilities, countermeasures and cyber security management. Vulnerabilities are addressed by considering connections to other computer systems, control of access, account management, physical protection and backups. Countermeasures for prevention, detection and mitigation of cyber attack are addressed. Management systems for cyber security are evaluated by considering various elements including policies and procedures, employee involvement, threat monitoring, security information, risk analysis, cyber security procedures, training, contractors, systems integrity, change management, incident reporting, response and investigation, and audits.

1.0 Connectivity

- 1.1 Are connections to other networks minimized?
- 1.2 Are connections to the Internet avoided where practicable?
- 1.3 Are wireless network access points secured?
- 1.4 Are dial-up modems avoided wherever possible?
- 1.5 Are dial-up modems appropriately secured?
- 1.6 Is modem use monitored?
- 1.7 Are dedicated connections to other computer systems avoided where possible?

2.0 Access

- 2.1 Are there policies and procedures to ensure there are no unattended, unsecure workstations?
- 2.2 Are there policies and procedures in place to manage backdoors?
- 2.3 Are computer facilities located away from the facility perimeter?
- 2.4 Are computer facilities sited away from remote areas?

3.0 Account Management

- 3.1 Is there an account management program?
- 3.2 Does the account management program establish levels of privilege?
- 3.3 Does the account management program employ minimum necessary access privileges?
- 3.4 Is there an account termination procedure?
- 3.5 Is there an account maintenance procedure?

4.0 Physical Protection

- 4.1 Is suitable physical protection provided for computer systems?
- 4.2 Are cables and wiring appropriately protected?
- 4.3 Are utilities, support, telecommunications and backup systems appropriately protected?

5.0 Backups

- 5.1 Are there backups for electrical power?
- 5.2 Are there backups for communications?
- 5.3 Are there backups for storage?

6.0 Prevention Countermeasures

- 6.1 Are system default configurations changed before commissioning?
- 6.2 Is there a policy on home use of PCs?
- 6.3 Are system vulnerability checks run after installation and maintenance work?
- 6.4 Is there a password policy and management program?
- 6.5 Are other authentication methods used?
- 6.6 Are screen-saver passwords used?
- 6.7 Are application log-outs used?
- 6.8 Is there a patch management program?
- 6.9 Are systems scanned for vulnerabilities?
- 6.10 Are precautions taken against war dialing and war driving?
- 6.11 Is war dialing used to identify unsecure or rogue modems?
- 6.12 Is encryption used?
- 6.13 Is encryption strong enough?
- 6.14 Are e-gaps or air gaps used?
- 6.15 Are modems secured?
- 6.16 Are wireless access points secured?
- 6.17 Are honeypots used?
- 6.18 Are precautions taken against sniffing?
- 6.19 Are precautions taken against spoofing?
- 6.20 Are firewalls used?
- 6.21 Is firewall activity audited?
- 6.22 Are DMZs used with bastion hosts?

- 6.23 Are VPNs used?
- 6.24 Are applications limited?
- 6.25 Are ports restricted on network devices?
- 6.26 Are maintenance operations secured?
- 6.27 Are countermeasures effective?
- 6.28 Are they maintained?

7.0 Detection Countermeasures

- 7.1 Are intrusion detection systems used?
- 7.2 Is there real time response to intrusion alarms?
- 7.3 Is IDS activity audited?
- 7.4 Is anti-malware used?
- 7.5 Is anti-malware updated regularly?

8.0 Mitigation Countermeasures

- 8.1 Is there an incident response program?
- 8.2 Is there an incident investigation program?
- 8.3 Is there a data recovery program?

9.0 Cyber Security Management System

- 9.1 Do cyber security policies and procedures exist?
- 9.2 Are cyber security policies and procedures followed?
- 9.3 Are cyber security policies and procedures revised as needed?
- 9.4 Are roles defined and responsibilities assigned?

- 9.5 Is authority provided?
- 9.6 Is supervision provided?
- 9.7 Are resources allocated?
- 9.8 Are people held accountable?

10.0 Employee Awareness, Education and Involvement

- 10.1 Is there security awareness training?
- 10.2 Does security awareness training cover:
 - 10.2.1 Password practices?
 - 10.2.2 Social engineering?
 - 10.2.3 Document security practices?
 - 10.2.4 Use of anti-malware?
- 10.3 Are security awareness reminders provided?
- 10.4 Is there regular refresher security awareness training?
- 10.5 Are contractors included in security awareness training?

11.0 Cyber Threat Monitoring

- 11.1 Does the facility stay abreast of new cyber threats?
- 11.2 Is there a patch management program?

12.0 Facility and System Information

- 12.1 Does the facility maintain a low profile?
- 12.2 Is information on company web sites controlled?
- 12.3 Are company newsletters, press releases, and articles screened for security violations?
- 12.4 Is sensitive trash shredded or incinerated?

- 12.5 Is computer equipment sent for sale or disposal sanitized?
- 12.6 Is access to sensitive information suitably controlled?
- 12.7 Do vendors control access to hardware and software design and operation information?
- 12.8 Is the public disclosure of information limited to what is absolutely necessary?
- 12.9 Is key information kept up-to-date?
- 12.10 Is there backup storage of electronic media?

13.0 Cyber Security Risk Analysis (CSRA)

- 13.1 Has a CSRA been performed?
- 13.2 Did the CSRA address relevant cyber threats?
- 13.3 Does the CSRA reflect the system as actually configured and operated?
- 13.4 Have recommendations from the CSRA been implemented?
- 13.5 Is the CSRA updated periodically?

14.0 Cyber Security Procedures

- 14.1 Are there written cyber security procedures?
- 14.2 Do cyber security procedures address:
 - 14.2.1 Personnel screening
 - 14.2.2 Information protection
 - 14.2.3 Document control
 - 14.2.4 Computer access
 - 14.2.5 Disposal of sensitive information
 - 14.2.6 Sanitization of storage media
- 14.3 Are cyber security procedures complete?
- 14.4 Are cyber security procedures written properly?
- 14.5 Are cyber security procedures followed?

- 14.6 Do cyber security procedures have a standard format and content?
- 14.7 Are cyber security procedures readily accessible by the people who need to use them?
- 14.8 Are cyber security procedures dated as needed?
- 14.9 Were affected personnel involved in the preparation of cyber security procedures?
- 14.10 Are old cyber security procedures purged?

15.0 Cyber Security Training

- 15.1 Are affected employees trained in cyber security matters, as appropriate?
- 15.2 Does training cover:
 - 15.2.1 Security awareness
 - 15.2.2 Security procedures
- 15.3 Are contractors included in training?
- 15.4 Is refresher training provided at appropriate intervals?

16.0 Contractors

- 16.1 Are the impacts of using contractors addressed?
- 16.2 Are subcontractors included?
- 16.3 Are contractor cyber security practices audited?
- 16.4 Is contractor access to computer systems controlled and limited?

17.0 Cyber Security Systems Integrity

- 17.1 Are cyber security systems properly designed, installed, operated, maintained, inspected and tested?
- 17.2 Are appropriate systems included?

- 17.3 Is the integrity of support systems, backup systems and utilities addressed?
- 17.4 Are both cyber and physical protection addressed?
- 17.5 Are procedures, employee training, and quality assurance addressed?
- 17.6 Are security-critical systems defined?

18.0 Cyber Management of Change

- 18.1 Are the possible security impacts of changes in the system considered in a management of change program?
- 18.2 Have types of change covered by cyber MOC been defined?
- 18.3 Are all pertinent changes reviewed?
- 18.4 Are suitable methods used to evaluate the impact of changes on cyber security?

19.0 Cyber Security Incident Reporting and Investigation

- 19.1 Is there an incident reporting and investigation policy and procedure?
- 19.2 Are suspicious events and breaches of the cyber security program reported and investigated?
- 19.3 Are applicable corrective actions taken?

20.0 Cyber Security Incident Response

- 20.1 Is there a written incident response plan?
- 20.2 Has the incident response been tested?
- 20.3 Is there an incident response team?
- 20.4 Are incident response team members appropriately trained?
- 20.5 Is there coordination with law enforcement and Federal agencies?
- 20.6 Are there emergency backups for support systems and utilities?

21.0 Cyber Security Audits

- 21.1 Are periodic audits conducted?
- 21.2 Do audits follow an acceptable procedure?
- 21.3 Is the audit protocol complete?
- 21.4 Is the protocol applied properly?
- 21.5 Are the audit results documented?
- 21.6 Are corrective actions taken?