AuditScripts

Server Security Policy

Version 2.3

EDITED BY KELLI K. TARALA

SECURITY enclave

Server Security Policy

Information Assurance Policy (v2.3)

Purpose:

Information assurance policies are created to set universal standards for organizations to facilitate data protection. They also align business goals and strategies with appropriate methods for technically or operationally protecting data. As business owners determine their requirements for protecting data, policies can define the control standards this organization will follow to meet those requirements.

Scope:

This information assurance policy applies to each of this organization's workforce members who have contact or potentially may have contact with this organization's data, applications, and computing resources. Workforce members include, but are not limited to, employees, contractors, vendors, service providers, volunteers, or any others who have or may come into contact with this organization's data, whether in a paid or unpaid capacity. Exceptions to this policy must be properly approved and documented in accordance with this organization's information assurance Control Exception Policy.

Standards References

CIS Critical Controls (v6.1):
1, 2, 3, 5, 9, 13, 14, 16, 18

NERC CIP (v5):
CIP-007-5

NIST 800 Series:
NIST SP-43
NIST SP-44
NIST SP 800-53
NIST SP 800-64
NIST SP 800-123
NIST SP 800-125
NIST SP 800-147
NIST SP 800-167

NIST 800-53 (rev4):

COBIT 5:
APO13, DSS05

ISO 27002:2013:
7.1, 7.2, 9.1, 9.2, 10.1, 10.3—7, 10.10, 11.1—6, 12.4, 12.6, 14.1

NIST Cybersecurity Framework (v1.0):
ID.AM-1, PR.DS-4, PR.DS-5
PR.DS-6

IIA GTAGs:
Not Applicable

PCI DSS (v3.2):
2, 3, 5, 6, 10, 11

HIPAA / HITECH:
164.308(a)(1), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5), 164.308(a)(6), 164.308(a)(7), 164.310(a)(1), 164.312(b)

GDPR:
Not Applicable

Statements:

1. An approved device configuration standard shall be maintained that contains documentation for all security configurations for each server version and type.
2. A secure system image shall be created and maintained for each of this organization's servers that include all necessary and approved software and configuration settings. This organization will attempt to maintain as few system images as necessary in order to maintain as much consistency between systems as possible.
3. Each server system must complete this organization's certification and accreditation process prior to being allowed on the production business network in accordance with this organization's Certification and Accreditation Policy.
4. All server systems visible to an untrusted network, including the internet, will routinely be reevaluated for business purposes and moved to a trusted network if possible.
5. Procedures shall be maintained which detail the specific server security configuration standards necessary to protect each system. These procedures shall be based on the classification levels defined in this organization's Data Classification Policy.
6. At least one data owner and data custodian shall be defined for each of this organization's servers. Data owners will work with data custodians to define classification levels, provide necessary resources for the system, and maintain the system in accordance with this organization's Data Classification Policy and Risk Management Policy.
7. If a data owner or data custodian cannot be determined for a particular system or if appropriate resources cannot be allocated to protect the system, then that system shall be decommissioned in accordance with this organization's System Decommissioning and Data Destruction Policy
8. Physical and environmental security controls shall be implemented for each of this organization's servers in accordance with this organization's Physical Security Policy and Environmental Security Policy.
9. An up-to-date inventory of all production and test server systems will be maintained at all times in accordance with this organization's Risk Management Policy. This inventory will include, at a minimum, information regarding the following: (a) The system's hardware configuration; (b) All approved software installations; (c) All authorized system user accounts; (d) All file access controls and user right assignments; (e) All network based access control lists; (f) All authorized running services; and (g) All listening network ports.
10. Each of this organization's servers shall have appropriate and approved file and network-based access control lists inventoried and configured and file integrity assessment controls in accordance with this organization's Access Control and Authorization Policy, Account and Identity Management Policy, and Network Security Policy.
11. All critical services such as Domain Naming Services, email, and other business-critical services will be installed and maintained on separate physical or logical hosts.
12. An application firewall will be installed in front of all critical servers and logging of critical events and alerts will be completed in accordance with this organization's Logging and Monitoring Policy.
13. Only those authorized running services and listening network ports which have been inventoried by the server's data owners and data custodians shall be running on any individual server in accordance with this organization's Network Security Policy.
14. Each system shall run the latest tested, approved and updated system software for both the server's operating system and all applications installed on the system in accordance with this organization's Software Update Policy.

15. Application firewalls shall be maintained in front of all web based applications in order to limit the effectiveness of attacks against the application. This system shall be updated on a regular basis with signatures of new or emerging attacks and shall be configured to both block and alert this organization when attempts are made to attack the web applications being protected by the system. This will be completed in accordance with this organization's Network Security Policy.
16. Vulnerability scans shall be performed on a regular basis on each of this organization's servers in accordance with this organization's Vulnerability Management Policy and the classification level of the server being scanned.
17. Penetration tests shall be performed on a regular basis on each of this organization's servers in accordance with this organization's Penetration Testing Policy and the classification level of the server being scanned.
18. Only authorized user accounts shall be configured and utilized on each of this organization's servers in accordance with the inventory approved for each server and this organization's Account and Identity Management Policy.
19. Administrator, root, or other superuser account rights will only be granted to servers when the use of non-elevated system accounts will not serve the same purpose. As with other user accounts, these accounts shall be approved, inventoried, and utilized in accordance with this organization's Account and Identity Management Policy.
20. Remote administration shall only be performed on systems where it has been authorized by the system's data owner. All approved remote administration shall be performed over properly encrypted channels using non-generic user accounts in accordance with this organization's Account and Identity Management Policy.
21. Centrally managed logging and monitoring shall be performed on each of this organization's server systems in accordance with this organization's Logging and Monitoring Policy, Auditing and Assessment Policy, and Network Security Policy. This monitoring shall be performed for the purposes of performance management, incident management, and change management.
22. Backups of each system shall be performed on a regular basis in accordance with this organization's Data Backup and Archiving Policy. These backups shall be performed of each server's operating system, application code, system and application configurations, and business data.
23. A test server system, which is a mirror of the production server system, shall exist for each of this organization's servers. This test version of the system must be kept in a trusted state off of this organization's production network.
24. A detailed business continuity and disaster recovery plan shall be documented, tested, and maintained for each of this organization's servers in accordance with this organization's Business Continuity and Disaster Recovery Policy.
25. Once a server's data owner has determined that the system is no longer necessary to meet this organization's business goals, it shall be decommissioned in accordance with this organization's System Decommissioning and Data Destruction Policy.
26. All server administrative tasks shall be conducted on a secured system exclusively for that purpose. Common business tasks such as word processing, internet access, and email shall be done from a standard business system in accordance with this organization's Access Control and Authorization Policy.
27. Each of this organization's computer users shall be educated on proper methods for understanding data and system risks in accordance with this organization's Training, Education, and Awareness Policy. This training shall include training for all classes of system users, including, but not limited to general system users, incident handlers, managers, and executives.

28. Exceptions to this policy shall be managed and maintained by following the processes outlined by this organization's Configuration Management and Change Management Policy and Control Exception Policy.

Assurance:

In order to ensure continued compliance with this policy, this organization will train all workforce members on their responsibilities that align with this policy. This training will consist of an initial education upon affiliating with this organization as well as continued education events on a regular basis in accordance with this organization's standards for training and education.

In addition, this organization shall implement an ongoing audit program. This audit program will adhere to this organization's policies and standards for auditing which shall reflect industry standards, practices, and ethics in this area. All levels of workforce members shall engage in this assurance effort, and they will not be limited to a formal internal audit group. Any workforce member who notices non-compliance with this policy shall notify the appropriate business owners of the deficiencies that exist.

Sanctions:

Any workforce member discovered violating this policy may be subject to disciplinary measures, up to and possibly including termination of employment or breach of contract with this organization. For employees, this disciplinary measure shall be administered by this organization's Human Resources Department in accordance with all human resource policies. For other workforce members, this disciplinary measure may result in a breach of contract or service level with this organization and therefore appropriate sanctions will be applied as per the agreed upon contractual terms by the purchasing representative or business process owner.

Administrative:

The Chief Executive Officer of this organization has the responsibility for the overall administration of this policy. Establishment of the administrative procedures for the compliance with Corporate Policies is the responsibility of the officers and the managers of this organization and its business units.

Definitions:

For further clarification on the terminology and definition of terms used within this document, please refer to this organization's published glossary of terms associated with this document.

Revision History:

Title and Version Number:	Server Security Policy
Status and publication date:	In draft
Last Formal Review:	
Superseded Documents:	All local policies
Related Documents:	Access Control and Authorization Policy Account and Identity Management Policy Auditing and Assessment Policy Business Continuity and Disaster Recovery Policy Certification and Accreditation Policy Configuration Management and Change Management Policy Control Exception Policy Data Backup and Archiving Policy Data Classification Policy Environmental Security Policy Logging and Monitoring Policy Network Security Policy Penetration Testing Policy Physical Security Policy Risk Management Policy Software Update Policy System Decommissioning and Data Destruction Policy Training, Education, and Awareness Policy Vulnerability Management Policy

Signature:

Prepared By:	Approved By: