|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Standards | | | | | |
| Template Management Standard | | | | | |
| STD # | STD-001 | Effective Date | MM/DD/YYY | Email | policy@informationshield.com |
| Version | 1.0 | Contact | Author | Phone | 888.641.0500 |

Table of Contents

[Purpose 1](#_Toc496181327)

[Scope 1](#_Toc496181328)

[Standard 1](#_Toc496181329)

[Standard Section 1 1](#_Toc496181330)

[Standard Section 2 1](#_Toc496181331)

[Standard Section 2 1](#_Toc496181332)

[References 2](#_Toc496181333)

[Approval and Ownership 2](#_Toc496181334)

[Revision History 2](#_Toc496181335)

Purpose

[Description of the purpose of this standard as it applies to protecting company X information.]

This standard defines the specific requirements to support Company X policy. This example is used to illustrate a standard to support system audit logging.

Scope

[Defines the organizational roles, systems or risk-domains where this policy applies.]

This standard applies to all Company X computer and communication systems that produce audit logs. The target audience of this standard is any Company X employee or third party responsible for managing information systems.

Standard

### Low Impact Systems

* 1. **System Log Contents -** All production operating systems and application systems must include logs that record, at a minimum:
     1. User session activity including user IDs,
     2. User logon date and time,
     3. User logoff date and time,
     4. User applications invoked,
     5. System changes to critical application system files,
     6. System changes to the privileges of users, and
     7. System start-ups and shut-downs.

### Medium Impact Systems

* 1. **System Log Contents -** All production operating systems and application systems classified as “medium” must include logs that record, at a minimum:
     1. All events from Low Impact systems, plus:
     2. Password guessing attempts,
     3. Attempts to use privileges that are not authorized,
     4. Failed Logon attempts,
     5. Changes to system services
     6. All Privileged User ID system commands; (Administrator Role)
     7. Modifications to production application software, and
     8. Modifications to system software.

### High Impact Systems

* 1. **System Log Contents -** All production operating systems and application systems classified as “high” must include logs that record, at a minimum:
     1. All events from Low and Medium Impact systems, plus:
     2. Activation and de-activation anti-virus systems and intrusion detection systems.
     3. Access to System Logs
     4. Initialization or pausing of System Logs

References

CPL: 15-01 Log Management and Monitoring Policy

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |