|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| System Planning and Acceptance Policy | | | | | |
| Policy # | CPL: 11-02 | Effective Date | 04/01/2013 | Email | policy@informationshield.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888.641.0500 |

Table of Contents

[Purpose 1](#_Toc385430276)

[Scope 1](#_Toc385430277)

[Policy 1](#_Toc385430278)

[Capacity Management 1](#_Toc385430279)

[System Acceptance 2](#_Toc385430280)

[Security of System Documentation 3](#_Toc385430281)

[Violations 4](#_Toc385430282)

[Definitions 4](#_Toc385430283)

[References 5](#_Toc385430284)

[Related Documents 5](#_Toc385430285)

[Approval and Ownership 5](#_Toc385430286)

[Revision History 5](#_Toc385430287)

Purpose

This policy defines the requirements for planning and for managing the capacity of Company X information processing resources.

A great emphasis should be placed on the continuous operation and availability of information systems, especially for an organization where any processing interruption can have catastrophic effects on the business or its customers. Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

Scope

This policy applies to all technology equipment that processes, stores, or transmits Company X information in any Company X facility or third-party facility on behalf of Company X, with a target audience of IT employees and executive management.

Policy

### Capacity Management

**Requirements** - Capacity requirements must be identified for each new and ongoing activity that requires the use of Company X information technology resources.

**Tuning and Monitoring** - System tuning and monitoring must be applied to all Company X information technology resources.

**Future Projections** - Projections of future capacity requirements must consider new business and system requirements and current and projected trends in the Company X information processing capabilities.

**Key Resources** - Company X management must monitor the utilization of key system resources, especially those with long procurement lead times or high costs.

**Trending** - Company X management must identify trends in usage, particularly in relation to business applications or management information system tools.

**System Security Status Tools** - Every multi-user system must include sufficient automated tools to assist the Security Administrator in verifying the security status of the computer and must include mechanisms for the correction of security problems.

**User Processes, Sessions, And Files** - Company X systems administration staff may, at any time and without notice, alter the priority of, or terminate the execution of, any user process that it believes is consuming excessive system resources or is significantly degrading system response time, terminate user sessions or connections if this usage is deemed to be in violation of security policies or consuming excessive system resources, or remove or compress user disk files if it believes these files consume excessive disk space.

**Systems Expertise** - Critical computer and communications expertise must be possessed by at least two immediately available persons.

### System Acceptance

**Security Impact Statements** - Prior to being placed into production use, each new, or significantly modified, or enhanced business application system must include a brief security impact statement that has been prepared according to standard procedures.

**Privacy Impact Reviews** - Every major systems development or enhancement project that could materially affect the privacy of individuals must be reviewed in advance by an independent committee, which must determine whether individuals will be placed at risk or at a disadvantage as a result of the project. If the committee determines that this may happen, they must then recommend remedial measures, perhaps including cancellation of the project.

**Performance** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include performance requirements.

**Capacity** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include computer capacity requirements.

**Recovery and Restart** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include error recovery and restart procedures.

**Contingency Plans** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include contingency plans.

**Operating Procedures** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include the preparation and testing of routine operating procedures to defined standards.

**Manual Procedures** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include effective manual procedures.

**System Impact** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include evidence that installation of the new system will not adversely affect existing systems at any time.

**Training** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include training in the operation or use of new or revised systems.

**Acceptance Criteria – Usability** - The acceptance criteria for new Company X information systems, upgrades, and the implementation of new versions must include ease of use.

**Testing** - Appropriate tests must be performed to confirm that all acceptance criteria have been fully satisfied.

**End-User System Development** - All software that handles sensitive, critical, or valuable information, and that has been developed by end users, must have its controls approved by the Information Security Department prior to being used for production processing.

**Software Conversion Contingency Plans** - Whenever the implementation of new or significantly modified production software introduces potential problems that could cause a loss to Company X of over $1,000,000, management must prepare a conversion-related contingency plan that reflects ways to insure continued service to potentially-affected users.

**User Acceptance Of Information Security Measures** - All information security controls must be both accepted and supported by the people who are monitored by and work with the controls.

### Security of System Documentation

**Document Classification** - All Company X computer related documentation is confidential, and must be treated with the corresponding level of control for this type of information.

**Documentation Release** - Prior to being released to third parties, all documentation that describes Company X information systems or systems procedures must be reviewed and approved by the Information Security Manager.

**Non-Business Use Of Organization Information** — Company X information (product specifications, databases, mailing lists, internal software, computer documentation, etc.) must only be used for the business purposes specifically allowed by management. Use of these information resources for any other purpose will be permitted only after written permission has been granted by the designated Owner of the information.

**Access To Media Libraries** - Access to magnetic tape, disk, and documentation libraries in the computer center must be restricted to workers whose job responsibilities require their presence in these areas.

**System Documentation on a Public Network** — All Company X system documentation held or provided on a public network must be protected against unauthorized access.

**Secret IDs or Passwords** - Developers must not build or deploy secret user IDs or passwords that have special privileges, and that are not clearly described in the generally available system documentation.

(Note: The following policies are related to NIST SA-5)

**Backups** - Monthly backups of information system documentation including security-related documentation must be conducted.

**Access Attempts** - Attempts to obtain information system documentation when such documentation is either unavailable or nonexistent must be documented.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

**Capacity Planning** - The process of determining the information processing capacity needed by an organization to meet changing demands for its products or services.

**Custodian** - Guardian or caretaker of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

**Emergency Change** - When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

**Owner** - The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

**Partner –** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**Privacy Impact Assessment** - An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Security Impact Analysis** - The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

**System Baseline** - The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

**System Acceptance, User Acceptance** - The demonstrable willingness within a user group to employ information technology for the tasks it is designed to support.

**Trusted Computer System** - An information system employing sufficient hardware and software assurance measures to allow simultaneous processing of a range of sensitive information.

**User -** Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

CPL: 11.02 System Planning and Acceptance

ISO 27002: 14.1 Security requirements of information systems

HIPAA: Organizational Requirements 164.314 (R)

PCI 2.2 Security Configuration Standards

NIST: Planning (PL)

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | 04/01/2013 |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | 04/01/2013 |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | 04/01/2013 | 04/01/2014 |  |
|  |  |  |  |  |