Zenventory, LLC

Change Management Policy

Effective Date 07/21/2022

Table of Contents

PURPOSE

This policy defines the requirements for managing changes to any Zenventory computer and communications system.

SCOPE

This policy applies to all information security analysts and system administrators responsible for the maintenance of Zenventory computer and communications systems.

POLICY

Authorization and Review

Production Operating System Changes - Extensions, modifications, or replacements to production operating system software must be made only if the written approval of the CEO or Directory of Technology has been received in advance.

Change Approval – All changes to Zenventory information systems equipment must be authorized by the CEO or Directory of Technology.

Security Considerations For Production System Changes - Prior to cut-over, every non-emergency change to production systems must be shown to be consistent with the information security architecture and approved by management as part of the formal change control process.

Procedures

Change Control Procedure - All computer and communications systems used for production processing at Zenventory must employ a formal change control procedure to authorize all significant changes to software, hardware, communications networks, and related procedures.

Production Change Personnel - Zenventory production data and production computer programs must be changed only by authorized people according to established procedures.

Systems Administrators Install/Update Server Software - Only authorized Systems Administrators are permitted to install and/or update software on Zenventory servers or servers hosting data.

Back-Off Procedures - Adequate back-off procedures, which permit information processing activities to quickly and expediently revert to conditions in effect prior to the most recent change in software, must be developed for all changes to production systems software and production application software.

Production Information System Change Implementation - All non-emergency production information systems changes must be communicated to affected resellers at least two weeks prior to the change. This section does not apply to regularly scheduled releases.

Change Testing - Operational Functionality - Prior to release to production all changes must be tested for operational functionality.

Change Documentation

Change Log On Every Server - Zenventory run servers shall have a log which details changes. At a minimum, this log must indicate the date, the Systems Administrator making the change, and the server component changed. Changes shall also be documented in product management systems such as JIRA.

Change Log Access – Zenventory follows the Principles of Least Privilege. As such, System access controls must be defined so that only authorized persons can make changes to production applications and/or change control records.

Patches and Updates

Security Patch Installation - All Zenventory computer and communications system components and software must have the latest vendor-supplied security patches installed.

Security Patch Installation Timing - All critical new security patches must be installed on Zenventory computer and communications systems within one month or receipt.

Software Patches, Bug Fixes, And Upgrades - All Zenventory networked production systems must have an adequately-staffed process for expediently and regularly reviewing, categorizing and installing all newly released systems software patches, bug fixes, and upgrades.

Digital Signature And Source Approval For Patches - Systems Administrators are authorized to patch software only if the software is downloaded, or otherwise received, from a trusted and recognized source approved by the Information Security Department. All patch software which comes with a digital signature must have its digital signature positively verified prior to being installed.

Frequency Of Installing Non-Emergency Patches, Fixes, And Upgrades - Management in charge of every production information system at Zenventory must establish a time period for the non-emergency periodic installation of patches, fixes, and upgrades to software. This time period must be based on the checklist of considerations provided by the Information Security Department.

Documenting Reasons Why Patches And Fixes Were Not Installed - If a patch or fix is not installed due to application conflicts or other incompatibilities, the involved Systems Administrator must promptly document the reason and forward the documentation to the Information Security Department.

Review of Previous Exceptions - Any un-patched or unfixed vulnerabilities must be addressed and resolved to the satisfaction of the Information Security Manager during the next information security review.

Review and Testing

Security Patch Testing - All security patches must be tested before they are installed on Zenventory production computer and communications systems. This must include, but not limited to the validation of all input to prevent cross-site scripting, injection flaws, and malicious file execution, proper error handling, secure cryptographic storage, secure communications, and proper role-based access control.

Development Testing For Software Patches, Fixes, And Updates - Vendor-supplied software patches, fixes, and updates must not be installed on any Zenventory production system unless they have first been tested in a development environment according to the requirements of the Systems Development Methodology.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Zenventory reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Zenventory 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, Zenventory reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

DEFINITIONS

Change - Any modification to the information processing infrastructure that is a result of:
- An implementation of new functionality.
- An interruption of service.
- A repair of existing functionality.
- A removal of existing functionality.

Change Management - The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

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 Zenventory who is contractually bound to provide some form of service to Company X.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

Scheduled Change – A modification to the information processing infrastructure where formal notification was submitted, reviewed, and approved in advance of the change being made.

Unscheduled Change – A modification to the information processing infrastructure where formal notification was not submitted, reviewed, and approved in advance of the change being made. Unscheduled changes may be implemented to maintain system integrity and security in a timely manner to prevent an emergency situation.

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

REFERENCES

CPL: 11.4 Change Management
ISO/IEC 27002 – 12.1.2 Change management
NIST: CM-3 Configuration Change Control
HIPAA: Security Management Process 164.308(a)(1)
PCI-DSS: 6.4 Change Control Processes

REVISION HISTORY

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version	07/21/2022	07/21/2023	Jason Scronic