COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

INFORMATION TECHNOLOGY SYSTEMS ASSET MANAGEMENT GUIDELINE

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

ITRM Publication Version Control: It is the user's responsibility to ensure that he or she has the latest version of the ITRM publication. Questions should be directed to the Director of VITA's Policy, Practice and Architecture (PPA) Division. PPA will issue a Change Notice Alert when the publication is revised. The Alert will be posted on the VITA Web site. An email announcement of the Alert will be sent to the Agency Information Technology Resources (AITRs) at all state agencies and institutions, as well as other parties PPA considered interested in the publication's revision.

This chart contains a history of this ITRM publication's revisions:

Version	Date	Purpose of Revision
Original	04/27/2009	

Preface

Publication Designation

ITRM IT Systems Asset Management Guideline

Subject

Information Technology Systems Security

Effective Date

April 27, 2009

Scheduled Review

One (1) year from effective date

Authority

Code of Virginia § 2.2-603(F)
(Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO)

Scope

This *Guideline* is offered as guidance to all executive, legislative, and judicial branch, and independent State agencies and institutions of higher education (collectively referred to as "Agency") that manage, develop, purchase, and use information technology (IT) resources in the Commonwealth.

Purpose

To provide agencies with guidance in meeting COV Information Security Program requirements and in the development and implementation of the IT systems asset management component of their agency information security program.

General Responsibilities

(Italics indicate quote from the Code of Virginia)

Chief Information Officer

In accordance with *Code of Virginia* § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information*

Chief Information Security Officer

The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's IT systems and data.

IT Investment and Enterprise Solutions Directorate

In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the IT Investment and Enterprise Solutions Directorate the following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."

All Executive, Legislative, and Judicial Branch and Independent State Agencies

In accordance with §2.2-2009 of the *Code of Virginia*,, all executive, legislative, and judicial branch and independent State agencies and institutions of higher education are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines that address security of state government electronic information from unauthorized uses, intrusions or other security threats issued by the Chief Information Officer of the Commonwealth.

Definitions

Agency - All executive, legislative, and judicial branch and independent State agencies and institutions of higher education that manage, develop, purchase, and use IT resources in the Commonwealth of Virginia (COV).

CISO - Chief Information Security Officer – The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of COV IT systems and data.

Data - An arrangement of numbers, characters, and/or images that represent concepts symbolically.

Data Owner - An agency Manager, designated by the Agency Head or Information Security Officer, who is responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data.

Electronic Information - Any information stored in a format that enables it to be read, processed, manipulated, or transmitted by an IT system.

Government Electronic Information - Electronic information owned or held by COV.

ISO – Information Security Officer - The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's IT security program.

IT System - An interconnected set of IT resources and data under the same direct management control.

Information Technology (IT) - Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Security - The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

Information Technology (IT) Security Audit - An independent review and examination of an IT system's policy, records, and activities. The purpose of the IT security audit is to assess the adequacy of IT system controls and compliance with established IT security policy and procedures.

Least Privilege - The minimum level of data, functions, and capabilities necessary to perform a user's duties.

Risk - The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Risk Assessment (RA) - The process of identifying and evaluating risks so as to assess their potential impact.

Risk Mitigation - The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Sensitivity - A measurement of adverse affect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled that compromise of IT systems and data with respect to confidentiality, integrity, and/or availability could cause. IT systems and data are sensitive in direct proportion to the materiality of the adverse effect caused by their compromise.

Sensitivity Classification - The process of determining whether and to what degree IT systems and data are sensitive.

Separation of Duties - Assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

Threat - Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data and/or denial of service by exploiting vulnerability.

Vulnerability*:* A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Related ITRM Policy and Standards

Current version of COV ITRM Security Policy

Current version of COV ITRM Security Standard

Current version of COV ITRM Security Audit Standard

Current version of COV ITRM Removal of Commonwealth Data from State Electronic Equipment Standard

TABLE OF CONTENTS

1 Introduction

This Guideline presents a methodology and guidance that agencies can use in developing and implementing the IT systems asset management component of their agency information security program. This guidance supports the Commonwealth's Information Security Program as defined in the current version of the Commonwealth of Virginia Information Technology Resource Management (COV ITRM) Security Policy and related COV ITRM security standards.

The function of the Security Policy is to define the overall COV Information Security Program, while the standards define the minimal COV Information Security requirements that must be included in agency information security programs. Agencies are not required to use the methodologies in guidelines, and may use methodologies from other sources or develop their own, provided that they meet the requirements identified in COV ITRM security related standards. The current version of COV ITRM Information Security Standard is hereinafter referred to as the "Standard" in this document.

Additional agency guidance relative to the financial aspects of fixed asset management including IT assets can be found in the Department of Accounts Commonwealth Accounting Policies and Procedures (CAPP) Manual.

2 IT Asset Management

IT Asset Management is an important business practice that involves maintaining an accurate inventory, licensing information, maintenance, and protection of hardware and software assets utilized by an agency. Understanding what IT assets are deployed in an agency's environment will help optimize the use of IT assets throughout the agency. An agency may find that their existing fixed asset control program used to manage all agency assets is sufficient to address IT asset control, while another agency may need to develop a more specific IT asset control program. This document provides guidance on the steps that can be taken to protect COV IT systems and data by managing the IT assets utilized by the COV in a planned, organized, and secure fashion. Appendix A contains the Example IT Asset Management Policy that incorporates the methodologies contained in this document. This component of the COV Information Security Program addresses the following three areas:

- IT Hardware Asset Control
- IT Software Asset Control
- Configuration Management and Change Control

3 IT Hardware Asset Control

The Standard requires agencies to "…control and collect information about IT assets". Any IT hardware asset that has value to the agency, that requires ongoing maintenance and support, or creates potential risk in terms of financial loss, data loss or exposure must be documented and controlled to meet COV security requirements.

Agencies need to address the following areas related to IT hardware:

- IT Hardware Asset Removal Control
- Personal IT Hardware Assets
- Data Removal from IT Hardware Assets
- Inventory of agency or agency leased IT Hardware Assets

3.1 IT Asset Hardware Removal Control

Each agency must determine and document whether, and in what circumstances, to permit the removal of IT hardware assets from premises that house COV IT systems and data. Removal of IT hardware assets should be based on the agency's unique operating environment and needs. Each agency should document business needs for allowing the removal of IT hardware assets from a COV work environment, and identify corresponding controls. Safeguards should be identified and documented by each agency to protect IT hardware assets and data when IT hardware assets are to be removed from premises. See Appendix A for the Example IT Asset Management Policy.

3.2 Personal IT Hardware Assets

Each agency or their service provider must determine and document whether personal IT hardware assets should be allowed onto premises that house COV IT systems and data based on the agency's unique operating environment and needs. Personal IT hardware assets should be prohibited unless there is an identified unique business need, which should be documented to include the need, risks, controls and unmitigated risks.

As stated in the Standard, agencies must "….prohibit the connection of any non-COV owned data storage media or device to a COV-owned network, unless the connection is to a segmented guest network. This prohibition, at the agency's discretion, need not apply to an approved vendor providing operational IT support services under contract."

"Note: Such media include, but are not limited to, USB drives, cell phones, personal digital assistants, desktops, laptops, and digital music players owned by employees, contractors, and/or students."

3.3 Data Removal from IT Hardware Assets

Commonwealth data must be removed from electronic media in accordance with the current version of the *Removal of Commonwealth Data from State Electronic Equipment Standard (ITRM SEC514).* "All electronic storage media shall have all Commonwealth data properly removed prior to surplus, transfer, trade-in, disposal, or replacement." The primary methods for removal of data from IT hardware assets include overwriting, degaussing and/or physical destruction.

See the current versions of the *Removal of Commonwealth Data from State Electronic Equipment Standard* (ITRM SEC514) and the *Data Protection Guideline* (ITRM SEC507) for more information on approved means of data removal.

3.4 Inventory of IT Hardware Assets

Agencies need an inventory and/or access to an inventory of the IT hardware assets used to support their mission and automated solutions. An agency and/or its service provider must know what IT hardware assets they have and where those assets are located in order to protect them. When determining what information to track for a particular asset, consider the following:

1. Specific information pertinent to the particular hardware asset
2. Physical location
3. Unique identifier of the asset
4. Support contract and information

Appendix B contains the Example and Template IT Hardware Asset Inventory.

Agencies and/or service providers should address labeling IT hardware assets. Labeled assets assist when troubleshooting problems, tracking and identifying inventory, and recovering lost or stolen IT hardware assets such as laptops and personal digital assistants (PDA's). Appendix C contains the Example and Template IT Hardware Asset Label. When an IT hardware asset is being moved or transferred from one location or responsible party to another, both parties should sign a log indicating acknowledgement of the transfer.

4 IT Software Asset Control

The Standard requires agencies to "…control and collect information about IT Assets" as well as "…protect against use of computer software in violation of applicable laws." This section of the Standard requires agencies to comply with software licensing requirements, and document software license management practices.

Each agency and/or their service provider should address distribution, purchase, audit, and removal of the licenses used in day-to-day business. Properly tracking licenses facilitates efficient use of resources and reduces the probability of violating licensing agreements and laws.

Agencies need to address the following areas related to IT software:

- Software Use Practices
- Software License Management Practices
- Software Asset Inventory

4.1 Software Use

The Standard requires each agency or its service provider "...document software license management practices that address the following components, at a minimum:

- Require the use of only approved software on IT systems.
- Agency or service provider should assess periodically whether all software is used in accordance with license agreements.

4.1.1 Use of Approved Software

Each agency should prohibit the installation of non-approved software by technical means as practical.

4.2 Software Management Practices

Each agency and/or their service provider should periodically assess whether software is used in accordance with license agreements. Agencies, in conjunction with any service providers, need to define responsibilities related to the activities associated with that periodic assessment. In addition to evaluating software license compliance, this assessment could include:

- Determining whether software is optimally deployed to eliminate waste
- Updating information to support software asset management functions, such as application maintenance cost analysis and upgrade budgeting
- Eliminating variation in software versions and supporting software updates

4.3 Software Asset Inventory

Agencies need an inventory or access to an inventory of the licensed software used to support their mission and automated solutions. Maintaining a complete licensed software asset inventory provides a tool to assess compliance with license agreements and whether the resources are being used efficiently and effectively. The information contained in this inventory should include product information, the business functions of the software, the users of the software, and the cost associated with the license.

5 Configuration Management and Change Control

Configuration management is defined as, “A management process for establishing and maintaining consistency of a product’s performance, functional, and physical attributes with its requirements, design and operational information throughout its life.”[1] Change control is a process in which changes to the configuration of an IT asset are to follow a structured procedure set forth by the agency in which changes are reviewed, approved, and documented.

The Standard states, “Configuration Management and Change Control requirements identify the steps necessary to document and monitor the configuration of IT systems, and to control changes to these items during their lifecycles. While the full extent of Configuration Management and Change Control is beyond the scope of this document, agencies are advised to institute structured practices in this area, based on industry standard frameworks such as the IT Infrastructure Library (ITIL) (www.itil.co.uk) or Control Objectives for Information and related Technology

[1] ANSI/EIA 649-1998, *National Consensus Standard for Configuration Management*

(COBIT)(www.isaca.org), among others." Agencies should refer to the current version of the Enterprise Technical Architecture Standard (ITRM Standard EA 225) for additional information.

ITIL provides very granular detailed service requirements while COBIT provides high-level control objectives. As a result, using COBIT as a framework for configuration management and change control requires substantially more development of a change control process on the part of an agency than does ITIL. Each agency should be aware of these differences as they evaluate whether to adopt ITIL-based requirements, COBIT-based requirements, or a hybrid of both for their configuration management and change control framework. To guide its configuration management and change control practices, each agency should select a framework that supports the mission, strategy, and environment of the organization.

Configuration management and change control should at a minimum, provide the agency with adequate assurance that changes made in day-to-day operations will not compromise the availability of the system or the confidentiality and/or the integrity of the data within a system, commensurate with sensitivity and risk. Ideally, configuration management and change control practices should be part of an overall service delivery and/or control framework that optimizes the delivery of IT services. Appendix D contains the Example Configuration Management Policy and Appendix E contains the Example Change Management Policy.

Appendix A. Example IT Asset Management Policy

PURPOSE: To document the agency policy on IT Asset Management.

SCOPE: All agency employees and business partners

ACRONYMS:	IT:	Information Technology
	CSA:	Citizen Services Agency

STATEMENTS OF POLICY:

1. IT users, to include, employees, business partners, and contract personnel shall not remove IT assets supplied by COV or its business partners from agency or company premises, except under the following conditions.
   a. IT assets assigned to employees, which may include laptop computers and Personal Digital Assistant (PDA) devices, may be removed from agency or company premises as deemed acceptable by the agency for the following reasons only:
      1. teleworking
      2. field work that is part of an assigned position

   b. Exceptions to this policy must be documented in writing and approved by the employee's supervisor and by the Agency Head. Documentation of exceptions shall include:
      i. The business or technical justification;
      ii. The scope of the exception, including quantification and duration (not to exceed one year);
      iii. A description of all risks associated with the exception;
      iv. Identification of controls to mitigate the risks; and
      v. Identification of any unmitigated risks associated with the exception.

2. IT users are responsible for safeguarding any IT assets they remove from the agency or business partner premises, including keeping these assets under their direct physical control whenever possible, and physically securing the assets (i.e., by means of lock and key) when they are not under the IT users direct physical control.

3. IT users must immediately report loss or theft of any assigned IT assets to their supervisor and as appropriate, to VITA within 24 hours of a known occurrence.

4. Unless stated otherwise within agency or facility policy, IT users are not allowed to bring personal IT assets into work locations that house COV IT systems and data; and personal IT assets may not be connected to the agency or business partner network.
   a. In general, connection of personal IT assets to networks provided by agency or business partner for guest or public access is allowed if deemed acceptable by the agency.

   b. Exceptions to this policy must be documented in writing and approved by the employee's supervisor and by the Agency Head. Documentations of exceptions shall include:
      i. The business or technical justification;
      ii. The scope of the exception, including quantification and duration (not to exceed one year);
      iii. A description of all risks associated with the exception;

iv. Identification of controls to mitigate the risks; and
v. Identification of all unmitigated risks associated with the exception.

5. "All electronic media containing Commonwealth data, whether stored on Commonwealth assets or that of a service provider, shall have all of that Commonwealth data securely removed from the electronic media as specified by current COV ITRM standards before the electronic media is surplused, transferred, traded-in, otherwise disposed of, or replaced.".

IT Software Asset Control

1. IT users shall only use agency and COV approved and appropriately licensed software on agency owned, leased, or COV provided IT Assets.

2. Installation of software that is not approved or appropriately licensed on agency owned, leased, or COV provided IT assets is prohibited.

3. No less than annually, the Agency Head or designee shall conduct an audit of software license distribution and reconciliation to verify and validate that all software used by the agency is appropriately licensed and approved.

Configuration Management and Change Control

1. Agency shall or shall require its service provider to document IT asset configuration and changes to asset configuration at all stages of the system development life cycle.

2. All changes to IT assets used by an agency shall be made in accordance with best practices as defined by the Information Technology Infrastructure Library (ITIL) framework and at a minimum include the following steps:
   - Initiate change request
   - Review and approve change
   - Build and test change
   - Create and document back up/back out plan
   - Implement change
   - Document change

AUTHORITY
REFERENCE: COV Information Security Policy, ITRM Policy

COV ITRM Information Security Standard

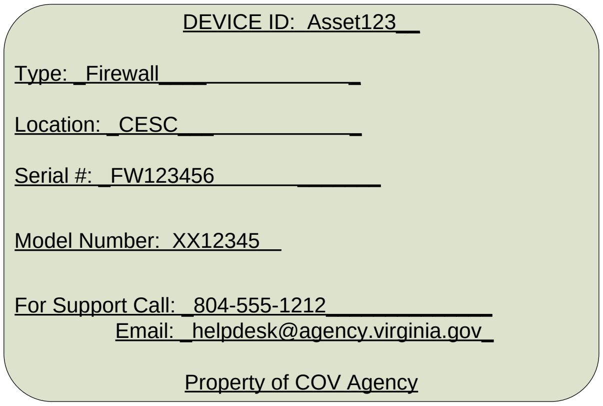
Appendix B. Example and Template IT Hardware Asset Inventory

Asset Type	Device ID	MAC Address	Serial #	O/S Level	CPU, Memory, Disk	Support Vendor	Model #	Install Date	Location	Floor
Server	S1021	00-0C-F1-56-98-AD	C-5499754	W2003 SP2	Quad 1.866Ghz, 4GB, 250GB	HP	BL465c	6/30/2008	CSA Datacenter	1st
Server	S1022	02-0C-F1-56-98-AA	C-5495625	W2003 SP2	Quad 1.866Ghz, 4GB, 250GB	HP	BL465c	6/30/2008	CSA Datacenter	2nd
Server	S1023	04-0C-F1-56-98-AB	C-5499931	W2003 SP2	Quad 1.866Ghz, 4GB, 250GB	HP	BL465c	6/30/2008	CSA Datacenter	1st
Server	S1024	00-0F-F1-56-98-AD	C-5704893	W2003 SP2	Quad 1.866Ghz, 4GB, 250GB	HP	BL465c	6/30/2008	CSA Datacenter	3rd
Server	S1025	12-0C-XX-56-98-AD	C-5704891	W2003 SP2	Quad 1.866Ghz, 4GB, 250GB	HP	BL465c	6/30/2008	CSA Datacenter	3rd
Server	S1027	07-0C-F1-S7-98-AD	C-5704892	W2003 SP2	Quad 1.866Ghz, 4GB, 250GB	HP	BL465c	6/30/2008	CSA Datacenter	2nd
Server	S1029	47-0C-F1-56-H5-AD	C-5704897	W2003 SP2	Quad 1.866Ghz, 4GB, 250GB	HP	BL465c	6/30/2008	CSA Datacenter	1st
Router	R101	00-0C-3F-56-98-CW	12559A	IOS 12.2	RAM 64 MB	Cisco	2600	6/30/2008	CSA Datacenter	
Router	R102	05-0C-F1-19-98-AD	12560A	IOS 12.2	RAM 64 MB	Cisco	2600	6/30/2008	Main Office	2nd
Router	R102	22-5C-F1-56-98-GD	12577A	IOS 12.2	RAM 64 MB	Cisco	2600	6/30/2008	Branch Office	3rd
Switch	SW09	08-0C-R7-56-98-SH	366051	IOS 14.1	RAM 16 MB SDRAM	Cisco	2960-24	6/30/2008	Main Office	1st
Switch	SW07	6H-AG-JK-D5-98-NM	367002	IOS 14.1	RAM 16 MB SDRAM	Cisco	2960-24	6/30/2008	Branch Office	1st
Firewall	FW107	0H-AY-F1-56-98-SH	995656	IOS 15.5	1.5 GB	Cisco	ASA5500	6/30/2008	CESC Datacenter	2nd
Firewall	FW109	00-K9-FA-65-98-H4	996554	IOS 15.5	1.5 GB	Cisco	ASA5500	6/30/2008	Main Office	2nd
Firewall	FW101	04-AG-F6-56-98-SR	982110	IOS 15.5	1.5 GB	Cisco	ASA5500	6/30/2008	Branch Office	2nd
Laptop	LT500	50-C3-F1-56-98-A9	AF6990577	XP Pro SP3	Intel Cel 2.86Ghz, 1GB, 60GB	HP	NC6400	07/10/2008	Main Office	3rd
Laptop	LT501	ND-0C-D2-56-98-A9	AF6950018	XP Pro SP3	Intel Cel 2.86Ghz, 1GB, 60GB	HP	NC6400	07/10/2008	Main Office	1st
Laptop	LT501	01-CF-17-59-98-AS	AF5520312	XP Pro SP3	Intel Cel 2.86Ghz, 1GB, 60GB	HP	NC6400	07/15/2008	Branch Office	3rd
Laptop	LT503	4D-02-H1-25-93-AM	AF6500900	XP Pro SP3	Intel Cel 2.86Ghz, 1GB, 60GB	HP	NC6400	07/15/2008	Branch Office	1st
Desktop	DT700	F2-0D-81-68-98-A8	DR270051	XP Pro SP3	Intel 2.86Ghz, 2GB, 120GB	HP	5800	07/10/2008	Main Office	3rd
Desktop	DT705	00-5T-F1-56-98-ZZ	DR265510	XP Pro SP3	Intel 2.86Ghz, 2GB, 120GB	HP	5800	07/15/2008	Branch Office	2nd
Desktop	DT706	04-ZC-F1-Z5-98-F7	DR995041	XP Pro SP3	Intel 2.86Ghz, 2GB, 120GB	HP	5800	07/15/2008	Branch Office	1st
Printer	P9051	07-22-26-56-H7-D3	401299A	05.004.02	128 Meg	HP	CLJ9500	07/10/2008	Main Office	3rd

Template IT Hardware Asset Inventory

Asset Type	Device ID	MAC Address	Serial #	O/S Level	CPU, Memory, Disk	Support Vendor	Model #	Install Date	Location	Floor

Appendix C. Example and Template IT Hardware Asset Label



DEVICE ID: Asset123__

Type: _Firewall____ _

Location: _CESC___ _

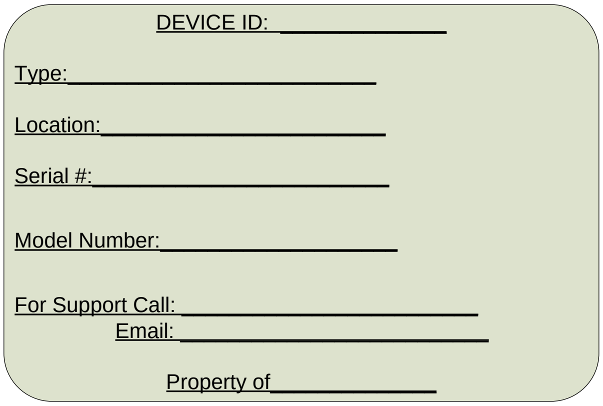
Serial #: _FW123456 _______

Model Number: XX12345

For Support Call: _804-555-1212_____________
Email: _helpdesk@agency.virginia.gov_

Property of COV Agency

Figure 1 Example IT Hardware Asset Label



DEVICE ID: ______________

Type:__________________________

Location:________________________

Serial #:_________________________

Model Number:____________________

For Support Call: _________________________
Email:__________________________

Property of______________

Figure 2 Template Hardware IT Asset Label

Appendix D. Example Configuration Management Policy

PURPOSE: To provide the framework and authority for the Citizen Services Agency (CSA) to maintain control of its information technology (IT) infrastructure components and to provide optimal service to CSA Customers at a justifiable cost.

SCOPE: All CSA Employees, CSA Customers, and Contractors

STATEMENT OF POLICY:

CSA has adopted the Information Technology Infrastructure Library (ITIL) framework and best practices to provide IT Service Support and IT Service Delivery management to CSA and CSA Customers. A relationship between the components of the infrastructure will be defined using a common software tool.

Terms

Configuration Management: The process of identifying and defining configuration items in a common data base, for the purpose of recording and reporting the status of these configuration items and requests for change (RFC).

Configuration Item (CI): A component of the IT Infrastructure or an item identifying an asset to be controlled.

IT Infrastructure: All components of the CSA statewide network of hardware; software; facilities; network communications; and scheduling processes.

Attributes: The characteristics and features of each CI.

Configuration Management Data Base (CMDB): A data base that contains all relevant detail of each CI and details of the important relationships between CIs.

Planning

- The Configuration Management owner will be clearly defined in the CSA organization.
- Configuration Management will plan for the accurate capture and maintenance of the CSA infrastructure configuration items.
- Configuration Management will define the location of current assets and their attributes in the CSA infrastructure to be managed.
- Configuration Management will provide data base support for other CSA IT support processes, such as: Incident, Release, Change, and Problem Management as well as the Service Desk function.

Identification

- The amount of details or attributes defined must remain at a manageable level. A realistic scope of recording of CIs will be planned that will allow the control to be maintained through the CSA Change Management process. Efforts and costs associated with capturing CI details should be compared with current and potential benefits.

- A method for accurate data collection of configuration items will be determined and executed to build a CMDB. A method for maintaining day-to-day changes to the CSA infrastructure must be implemented to keep the CMDB accurate.

- Relationships between the CIs that describe their interdependencies will be identified and recorded using the common software tool.

Control

- Configuration Management will implement procedures that will maintain the integrity of the data contained in the CMDB.

- The CMDB will be backed up on a regular basis and securely stored according to the CSA Data Protection and Data Recovery Policy.

- Updates and installations of infrastructure CIs will be recorded through Change Management and Release Management. The CMDB will be updated to reflect the specifications of the change.

- The CMDB will support the vital role of controlling software licenses used in the Commonwealth.

Status Accounting

- Historical status of each CI will be maintained throughout its life cycle. This historical status will support other Service Management activities, including, change control, Release Management, Problem Management, configuration audits, and service and financial planning.

- All changes to CSA infrastructure items must be authorized. A record of all authorized changes and enhancements is made on the CMDB.

Verification and Audit

- Configuration audits will be performed in areas of the infrastructure where unauthorized CIs are detected or when inconsistencies are discovered when an incident is reported.

- Prior to a major release or change, an audit of a specific configuration may be required to ensure that the Customer's environment matches the CMDB.

- Configuration audits will be performed to check the integrity of the CMDB with the physical state of the infrastructure CIs at least every 120 days.

Management Information

- Reports of detailed information on CIs will be provided as needed for documentation.

- Configuration Management will provide metric reports that provide detail lists for asset management, inquiries for license verification, maintenance renewal tracking, and budget planning, etc. that can be used by CSA management for decision-making processes.

Appendix E. Example Change Management Policy

PURPOSE: To provide the framework for the implementation and tracking of all changes that would impact the Citizen Services Agency (CSA) Information Technology. A change is any alteration to any component of the aforementioned CSA infrastructure of hardware, software, facilities, network communications, procedures, scheduling process or system documentation. CSA's Change Management practices are based upon the best practices defined by the Information Technology Infrastructure Library (ITIL) framework.

This policy outlines current Change Management practices, which are subject to revision to meet the evolving needs of the organization.

SCOPE: All CSA Employees and Contractors Supporting CSA

STATEMENT OF POLICY:

Change Management will be conducted throughout the CSA infrastructure using CSA's Change Management Application.

A Request for Change (RFC) falls into one of three categories:

1. **Normal –** A Normal Change is any change that can be planned, approved and scheduled prior to implementation.
   1.1 Submission before designated cutoff time
   1.2 Acceptance
   1.3 Classification
   1.4 Approval
   1.5 Implementation

2. **Emergency** – An Emergency Change is any change that requires immediate implementation to resolve system outages.
   2.1 Implementation
   2.2 Submission marked as Emergency
   2.3 Acceptance

3. **Critical** – A Critical Change is any change that does not meet the Normal or Emergency Change Request criteria. This type of change is to fix a known problem but has missed the normal Change Approval process and would need to be implemented before the next normal Change Approval period.
   3.1 Submission marked as Critical
   3.2 Acceptance
   3.3 Classification
   3.4 Approval
   3.5 Implementation

Roles and Responsibilities

Requester – responsible for submitting request through Change Management Application, attending the Change Management meeting for a Normal change request or have a representative present to discuss the request, and see that the change is performed and documented.

Operations Analysts - responsible for processing and posting of change request.

Relationship with Other Processes

Incident Management – required for the accurate and comprehensive recording of incident data in order to identify trends and ultimately root cause.

Problem Management – required for the correction of events that occur for which the cause is unknown.

Terms

Cutoff Time – A pre-defined time designed to allow for appropriate review and approval of a planned change.

Submission **-** A Request for Change (RFC) is submitted via electronic form using CSA's Change Management software. Requests are submitted to Change Management.