**IT Security Exception and Exemptions Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the IT Security Exception and Exemption Policy. This policy and procedure establishes the minimum requirements for the IT Security Exception and Exemption Policy.

This policy is intended to meet the requirements outlined in SEC501, Section 1.5 Exceptions to Security Requirements and Section 1.6 Exemptions from Applicability.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all sensitive “YOUR AGENCY NAME” systems

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The IT Security Exception and Exemptions Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the Exceptions to Security Requirements and Exemptions from Applicability requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs “YOUR AGENCY NAME” to meet these requirements.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |
| --- | --- | --- |
| **Roles** | Agency Head | Information Security Officer |
| **Tasks** |   |   |
| Request an exemption | A/R | I |
| Review request | I | A/R |

# STATEMENT OF POLICY

In accordance with SEC501, Exceptions to Security and Exemptions from Applicability, the “YOUR AGENCY NAME” Information Security Officer (ISO) shall approve or deny exceptions to any “YOUR AGENCY NAME” IT Security policy and/or procedure.

1. EXCEPTIONS TO SECURITY REQUIREMENTS
	1. While an exception may cover “YOUR AGENCY NAME” customer infrastructure, staff (“YOUR AGENCY NAME” and Business Partners) may not submit exceptions to the “YOUR AGENCY NAME” ISO on behalf of customer agencies. Customer agencies must understand and assume the risks posed by an exception by submitting a “YOUR AGENCY NAME” IT Security Policy & Standard Exception Request Form (Attachment A and included in SEC501). Denials of requests for exceptions may be appealed to the “YOUR AGENCY NAME” Agency Head through the “YOUR AGENCY NAME” ISO.
	2. The COV IT Security Standard is the overarching COV IT Security Standard for “YOUR AGENCY NAME”. In some instances, “YOUR AGENCY NAME” has created additional policies and procedures to provide more specificity to the COV IT Standards. If an Executive Director determines that compliance with any information security standards would adversely impact a business process of the agency, the Executive Director may request approval to deviate from a specific requirement by submitting the attached “YOUR AGENCY NAME” Security Policy & Procedure Exception Request Form to the agency ISO.
	3. The following steps must be used for completing the “YOUR AGENCY NAME” Security Policy & Procedure Exception Request Form:
		1. Each request for an exception must provide:
			1. Business or Technical Justification detailing the reasons for the exception including the “YOUR AGENCY NAME” Security Policy or Procedure for which the exception is being requested;
			2. Scope including quantification and requested duration (not to exceed one (1) year);
			3. Analysis of all associated risks;
			4. Explanation of the controls to mitigate the risks;
			5. Explanation of any residual risks; and
			6. Approval of the Agency Head or Executive Director of the organizational area requesting the exception. If the exception is for a customer agency, the Agency Head must sign indicating their approval of the exception and the assumption of the risks.
	4. The exception request form must be filled out, signed by both the requestor and the appropriate Executive Director or Agency Head of customer agency, and submitted to VITA Commonwealth Security and Risk Management. The form may be sent via email to CommonwealthSecurity@vita.virginia.gov by the Executive Director or Agency Head of customer agency. The requestor may submit with a copy to the Executive Director or Agency Head of customer agency.
	5. The ISO or designee will review the request and follow up with any questions or concerns and will notify the requestor of approval or denial.
	6. A written request for appeal of a denial shall be submitted to the CISO for transmission to the CIO.
2. EXEMPTIONS FROM APPLICABILITY
	1. The following are explicitly exempt from complying with the requirements defined in “YOUR AGENCY NAME” policies:
		1. Systems under development and/or experimental systems that do not create additional risk to production systems
		2. Surplus and retired systems

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO”““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

 [ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History |
| --- |
| Version | Date | Change Summary  |
| 1 | 08/08/2005 | Original |
| 2 | 01/20/2008 | Name changed from “*Security Policy Exception Policy and Procedure*.” Scoped expanded to include Business Partners and content amended to support an exception rather than an exemption process.  |
| 3 | 12/18/2008 | Clarity changes to Attachment 1: “YOUR AGENCY NAME” Security Policy & Procedure Temporary Exception Request FORM. |
| 4 | 06/17/2010 | Remove “Temporary” and “CISIAO” as referenced throughout the document. Also, replaced “unmitigated” with “residual” to align with Commonwealth Security Standard SEC501.  |
| 4.1 | 08/06/2010 | Updated link for COV ITRM Information Security Standard (SEC501-01). |
| 5 | 02/08/2013 | Administrative Changes |
| 6 | 07/01/2014 | Name changed and updated to conform to Information Security Standard SEC501 revision 8. Role matrix added |
| 7 | 11/19/202 | Formatting changes |

**Attachment 1:**

###

**VITA IT Security Policy & Standard Exception Request Form**

**Date of Request:** \_\_\_\_\_\_\_\_\_\_

**Requester:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Directorate**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Note: This request is for an exception(s) to a component of the “YOUR AGENCY NAME” Security policy and/or procedure(s) and approval of this request does not in any way address the feasibility of operational implementation. You are encouraged to check with your technical support staff prior to submitting this request.

1. Provide the **Business or Technical Justification:** *(Identify the “YOUR AGENCY NAME” Security Policy or Procedure for which exception is being requested*)

2. Describe the scope including quantification and requested duration (not to exceed one (1) year):

3. Describe all associated risks**:**

4. Identify the controls to mitigate the risks:

5. Identify all residual risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

Virginia Information Technologies Agency or Customer Agency Approval

Approved ­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Requesting Executive Director or Date

Agency Head of Customer Agency \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Name of Customer Agency

**Information Security Officer (ISO) Use Only**

Approved\_\_\_\_\_\_\_\_\_\_ Denied\_\_\_\_\_\_\_\_\_ Comments:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

ISO Date

**Requesting Executive Director or Agency Head of Customer Agency for Appeal Use Only:**

Approved for Appeal \_\_\_\_\_\_\_\_\_\_ Comments:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

Executive Director or Date

Agency Head of Customer Agency

**Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)**

Appeal Appeal

Approved\_\_\_\_\_\_\_\_\_\_ Denied\_\_\_\_\_\_\_Comments:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_

CIO Date