Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson
Commonwealth Information Security Officer

April 3, 2019

ISOAG April 3, 2019 Agenda

I. Welcome and Opening Remarks	Mike Watson, VITA
II. Intelligent Virtual Assistants	Dr. Michaela Iorga, NIST
III. Writing Policies and Procedures	Bob Auton, VITA
IV SAIC ISO Update	Grayson Walters, SAIC
V. Upcoming Events	Mike Watson, VITA

Upcoming Events

Virginia Information Technologies Agency

VITA Policies and Procedures Templates

Bob Auton
Centralized Information Security Services - VITA

April 3, 2019

CHAPTER 775 - An Act to amend and reenact § 2.2-2009 of the Code of Virginia, relating to the Virginia Information Technologies Agency; additional duties of CIO; cybersecurity review. Approved April 4, 2018

Relationship Management and Governance Directorate In accordance with the Code of Virginia § 2.2-2009 the CIO has assigned the Enterprise Solutions and Governance Directorate the following duties:

C. In addition to coordinating security audits as provided in subdivision B1, the CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency,…. Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairmen of the House Committee on Appropriations and the Senate Committee on Finance.

VITA policies and procedures background

The policy and procedures templates were prepared in 2014 and are based on SEC501 Revision 8. They are currently in the process of being revised.

The mandatory policy requirements for the 17 Families are included in the policies.

There are also 15 additional supplemental policies and procedures that have been prepared.

Location of the policies and procedure templates

The policies and procedures are located on VITA's IT Governance's ITRM Policies, Standards and Guidelines webpage

- Under the 'Tools and Templates' section

- Name: **SEC501 Policies and Procedure Templates**

Located at the following web address
http://www.vita.virginia.gov/it-governance/itrm-policies-standards/sec501-p--p-templates/

SEC 501 required policies

VITA CSRM - Logical Access Controls Policy
VITA CSRM - Security Awareness and Training Policy
VITA CSRM - IT Security Audit, Monitoring and Logging Policy
VITA CSRM - IT Security Assessment and Authorization Policy
VITA CSRM - IT Configuration Management Policy
VITA CSRM - IT Contingency Planning Policy
VITA CSRM - IT Identification and Authentication Policy
VITA CSRM - IT Incident Response Policy
VITA CSRM - IT System Maintenance Policy
VITA CSRM - IT Media Protection Policy
VITA CSRM - Physical and Environmental Protection Policy
VITA CSRM - IT System Security Planning Policy
VITA CSRM - IT Personnel Security Policy
VITA CSRM - IT Risk Assessment Policy
VITA CSRM - IT System and Services Acquisition Policy
VITA CSRM - IT System and Communications Protection Policy
VITA CSRM - IT System and Information Integrity Policy

Policy sections

Sections for each policy –

- PURPOSE
- SCOPE
- ACRONYMS
- DEFINITIONS
- BACKGROUND
- ROLES and RESPONSIBILITY
- STATEMENT OF POLICY
- ASSOCIATED PROCEDURES
- AUTHORITY REFERENCE
- OTHER REFERENCE
  - **Also Includes a Version History Table**

Roles and responsibilities for policy

ROLES and RESPONSIBILITY MATRIX FOR POLICY COMPONENT SECTION

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 the 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 and responsibilities chart

Example ***VITA's Business Impact Analysis Policy Roles & Responsibilities Chart***	Agency Head	Information Security Officer	Agency Continuity Coordinator	Agency Continuity Team	Agency Directors	Data and System Owners
Tasks						
Designate an Agency continuity coordinator		A/R				
Assign members to serve on continuity team					A/R	
Coordinate BIA and continuity plans			A	R		R
Develop a list of all business functions			I		A	R
Create MEF's and PBF's			I		A	R
Determine resources for MEF's and PBF's			I		A	R
Document RTO and RPO for MEF's and PBF's			I		A	R
Produce BIA			A			R
Review BIA on an annual basis			A	R	C	C
Review and approve BIA	A/R	C				

Supplemental policies and procedures

VITA CSRM - Business Impact Analysis Policy
VITA CSRM - Disaster Recovery Staffing Policy
VITA CSRM - Emergency Response Damage Assessment Procedure
VITA CSRM - Emergency Response Employee Communications Procedure
VITA CSRM - Enterprise Background Check Policy
VITA CSRM - Information Resource Acceptable Use Policy
VITA CSRM - Information Security Incident Reporting Procedure
VITA CSRM - Information Security Incident Response Procedure
VITA CSRM - Information Security Program Policy
VITA CSRM - Information Security Roles and Responsibilities Policy
VITA CSRM - IT Security Exception and Exemptions Policy
VITA CSRM - IT System and Communications Encryption Policy
VITA CSRM - IT System and Data Classification Policy
VITA CSRM - Mobile Device Access Controls Policy
VITA CSRM - Remote and Wireless Access Controls

Guidance provided by supplemental policies

The supplemental policies also have additional information that can be helpful –

An example is the *Information Security Incident Response Procedure* that has:

1. **ATTACHMENT A - Initial Response Checklist**
2. **ATTACHMENT B - Windows Forensics Checklist**
3. **ATTACHMENT C - Unix Forensic Command Log**
4. **ATTACHMENT D - Description of Evidence Form**
5. **ATTACHMENT E - Chain of Custody Form**

ATTACHMENT A - Initial Response Checklist

Contact Information

Your Contact Information

Name:	
Department:	
Telephone:	
Other Telephone:	
Email:	

Individual Reporting Incident

Name:	
Department:	
Telephone:	
Other Telephone:	
Email:	

Incident Detection

Type of Incident:	☐ Denial of Service ☐ Unauthorized Access ☐ Virus ☐ Unauthorized Use of Resources ☐ Hoax ☐ Theft of Intellectual Property ☐ Other:_____ _____ _____ _____

ATTACHMENT A - Initial Response Checklist

System Details

System Information:	
Make/Model of System:	
Operating System:	
Primary System User:	
System Admin:	
IP Address:	
Network Name:	
Modem Connection(Y/N)	
What Critical Information is contained on the system:	

ATTACHMENT A - Initial Response Checklist

Incident Containment

Is the incident still in progress or ongoing?	
Are you performing network Surveillance?	
Is the system still connected on network? If so, why is it still online? If not, who authorized removal? When will it be placed back online?	

Incident #:_____ Date:_____

Guidance provided by supplemental policies

Another example is the *Information Resource Acceptable Use Policy* that has:

ATTACHMENT A - Acknowledgement Of Acceptable Use Of IT Resources

ATTACHMENT B - Information Security Access Agreement

ATTACHMENT A - ACKNOWLEDGEMENT OF ACCEPTABLE USE OF IT RESOURCES

Acknowledgement Of Acceptable Use Of IT Resources

I understand and agree to abide by current and subsequent revisions to the VITA CSRM Information Resource Acceptable Use Policy and the Code of Virginia, Section 2.2-2827.

I understand that VITA has the right to monitor any and all aspects of their computer systems and networks, Internet access, and Email usage and that this information is a matter of public record and subject to inspection by the public and VITA management for all computer equipment provided by VITA. I further understand that users should have no expectation of privacy regarding Internet usage and sites visited or emails sent or received in such circumstances, even if the usage was for purely personal purposes.

My signature below acknowledges receipt of the VITA CSRM Information Resource Acceptable Use Policy.

Questions

Future ISOAG

May 1, 2019 @ CESC 1-4 p.m.

Speakers: Amy Luffey, ABC

Benjamin Gilbert, HDS

ISOAG meets the first Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk