***System and Services Acquisition Policy***

*ITC/ORG Name Here*

version 1.0

August 2021

## Document Review History

|  |  |  |
| --- | --- | --- |
| Date | Version | Reviewers |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Filename/Version | Author | Revision Description |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Contents**

[Document Review History i](#_30j0zll)

[Document Change History i](#_1fob9te)

[Introduction 1](#_3znysh7)

[Background 1](#_2et92p0)

[Purpose 1](#_tyjcwt)

[Scope and Applicability 1](#_3dy6vkm)

[System and Services Acquisition Policies 1](#_1t3h5sf)

[Allocation of Resources 2](#_4d34og8)

[System Development Life Cycle 2](#_2s8eyo1)

[Acquisition Process 2](#_17dp8vu)

[Information System Documentation 4](#_3rdcrjn)

[Security Engineering Principles 5](#_26in1rg)

[External Information System Services 5](#_lnxbz9)

[Developer Configuration Management 6](#_35nkun2)

[Developer Security Testing and Evaluation 7](#_1ksv4uv)

[Procedures 7](#_2jxsxqh)

[Resources 7](#_z337ya)

[Roles and Responsibilities 7](#_3j2qqm3)

[Train Personnel 8](#_1y810tw)

[Follow Up 8](#_4i7ojhp)

[Compliance 8](#_2xcytpi)

[Documentation Compliance Review 8](#_1ci93xb)

[Security Officer Documentation Compliance Review 8](#_3whwml4)

[Acronyms/Definitions 9](#_2bn6wsx)

[References 10](#_qsh70q)

[Forms (If applicable) 11](#_3as4poj)

# Introduction

## Background

This policy is authorized and in use by {{ORG Name}, hereafter referred to as {ORG Abbreviated Name}, as defined in the definition page of this document, and it applies to personnel, as defined in the definition page of this document. The confidentiality, integrity, and availability of information stored within the information systems of {{ORG ABBREVIATED NAME}} must be protected in order to comply with federal and state law, governing policies, and to preserve our reputation as a caretaker of sensitive information. System and services acquisition controls are in place to that new systems and processes introduced to the architecture are vetted properly and deployed in a manner consistent with the security architecture.

## Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information systems in use by {{ORG ABBREVIATED NAME}} by defining the processes related to the addition of systems and services within {ORG Abbreviated Name}.

## Scope and Applicability

This policy applies to all personnel, business processes and information systems managed by {{ORG ABBREVIATED NAME}}.

Exceptions

Any {{ORG ABBREVIATED NAME}} exceptions to this policy are documented in Appendix “A” of this document.

# System and Services Acquisition Policies

## (SA-2) Allocation of Resources

{{ORG ABBREVIATED NAME}} shall determine information security requirements for the information system or information system service in the mission/business process planning process. {{ORG ABBREVIATED NAME}} Security Officer determines, documents, and allocates the resources required to protect the information system or information system service as part of the capital planning and investment control process. Business Processes shall have a discrete line item for information security in {ORG Abbreviated Name} programming and budgeting documentation.

## (SA-3) System Development Life Cycle

{{ORG ABBREVIATED NAME}} Technology Staff shall manage the information system using criteria that incorporates information security considerations. The Security Officer shall define and document information security roles and responsibilities throughout the system development life cycle. The system development life cycle shall identify personnel having information security roles and responsibilities and integrate the {ORG Abbreviated Name} information security risk management process into system development life cycle activities.

## (SA-4) Acquisition Process

{{ORG ABBREVIATED NAME}} shall include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and {ORG Abbreviated Name} mission/business needs:

* Security functional requirements.
* Security strength requirements.
* Security assurance requirements.
* Security-related documentation requirements.
* Requirements for protecting security-related documentation.
* Description of the information system development environment and environment in which the system is intended to operate.
* Acceptance criteria.

## (SA-5) Information System Documentation

For externally developed systems, {{ORG ABBREVIATED NAME}} shall obtain administrator documentation for the information system, system component, or information system service that describes:

* Secure configuration, installation, and operation of the system, component, or service.
* Effective use and maintenance of security functions/mechanisms.
* Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

Additionally, {{ORG ABBREVIATED NAME}} shall obtain user documentation for the information system, system component, or information system service that describes:

* User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
* Methods for user interaction, which enables personnel to use the system, component, or service in a more secure manner.
* User responsibilities in maintaining the security of the system, component, or service.

{{ORG ABBREVIATED NAME}} shall document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and complete a risk assessment in response.

The documentation shall be protected as required, in accordance with the risk management strategy and distributed to appropriate personnel as needed.

## (SA-8) Security Engineering Principles

{{ORG ABBREVIATED NAME}} shall apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

## (SA-9) External Information System Services

{{ORG ABBREVIATED NAME}} shall require providers of external information system services to comply with {ORG Abbreviated Name} information security requirements and employ {{ORG ABBREVIATED NAME}} equivalent controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

{{ORG ABBREVIATED NAME}} shall define and document government oversight and user roles and responsibilities with regard to external information system services where necessary and employ processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

## (SA-10) Developer Configuration Management

{{ORG ABBREVIATED NAME}} requires the developer of the information system, system component, or information system service to:

* Perform configuration management during system, component, or service design, development, implementation, and/or operation~~.~~
* Document, manage, and control the integrity of changes to items as defined in Configuration Management Policy “Configuration Change Control.”
* Implement only {ORG Abbreviated Name} approved changes to the system, component, or service.
* Document approved changes to the system, component, or service and the potential security impacts of such changes.
* Track security flaws and flaw resolution within the system, component, or service and report findings to Security Officer.

## (SA-11) Developer Security Testing and Evaluation

{{ORG ABBREVIATED NAME}} shall require the developer of the information system, system component, or information system service to:

* Create and implement a security assessment plan.
* Perform unit, integration, system, and/or regression testing/evaluation at depth and coverage defined by {ORG ABBREVIATED NAME}}.
* Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.
* Implement a verifiable flaw remediation process.
* Correct flaws identified during security testing/evaluation.

## (SA-12) Supply Chain Protection

The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.

## (SA-13Trustworthiness

The organization:

* Describes the trustworthiness required in the [Assignment: organization-defined information system, information system component, or information system service] supporting its critical missions/business functions; and
* Implements [Assignment: organization-defined assurance overlay] to achieve such trustworthiness.

## (SA-14) Criticality Analysis

The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization-defined decision points in the system development life cycle].

## (SA-15) Development Process Standards and Tools

The organization:

* Requires the developer of the information system, system component, or information system service to follow a documented development process that:
* Identifies the standards and tools used in the development process;
* Documents the specific tool options and tool configurations used in the development process; and
* Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
* Reviews the development process, standards, tools, and tool options/configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [Assignment: organization-defined security requirements].

## (SA-16) Developer Provided Training

The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

## (SA-17) Developer Security Architecture and Design.

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

* Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;
* Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
* Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

## (SA-18) Tamper Resistance and Detection

Control: The organization implements a tamper protection program for the information system, system component, or information system service.

## (SA-21) Developer Screening

The organization requires that the developer of [Assignment: organization-defined information system, system component, or information system service]:

* Have appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and
* Satisfy [Assignment: organization-defined additional personnel screening criteria].

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
|  | Validate compliance on a {Time Period} basis. |
|  | Provide policy during new hire process and informs personnel of changes. |
|  |  |
|  |  |
|  |  |
|  |  |

## Train Personnel

Personnel are informed by a {{ORG Abbreviated Name} Human Resources} representative of this policy during the new-hire process and are incrementally informed when the policy changes.

## Follow Up

The products of this policy must be reviewed at least annually and when the {{ORG ABBREVIATED NAME} ’s} review indicates that updates are required.

## Compliance

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Documentation Compliance Review

All roles identified above must maintain documented proof of compliance for portions of this policy that are applicable to their responsibilities.

## Security Officer Documentation Compliance Review

The Executive Director will validate compliance with this policy on an annual basis.

# Acronyms/Definitions

|  |  |
| --- | --- |
| Acronym/Term | Definition |
| MC {ORG ABBREVIATED NAME} | Management Council of the Ohio Education Computer Network |
| Personnel | Employees, contractors, consultants, temporary workers, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

# Forms (If applicable)