System Development and Acceptance Policy

Purpose

The purpose of the (District/Organization) System Development and Acceptance Policy is to establish the rules for evaluating, developing, and/or deploying **Information Resources**.

Audience

The (District/Organization) System Development and Acceptance Policy applies to individuals who participate in the procurement, development, or operation of any (District/Organization) **Information Resource**.

Contents

[General](#_General)

[Secure Development](#_Secure_Development)

[System Acceptance](#_System_Acceptance)

Policy

### ****General****

* Applications created or deployed inside the (District/Organization) IT environment must follow a standardized application lifecycle established by management.
* Applications should be actively maintained and have periodic updates to address vulnerabilities. If an application is no longer maintained by the developer or another party, it must be evaluated for replacement.
* At the onset of the acquisition or design phase of an application deployment, the (District/Organization) Security Officer (or a delegate) must provide a list of required security controls based on the Secure Software Development Lifecycle Standard.
* Development, testing, and operational environments must be separated.
* Separation of duties must exist between personnel assigned to the development/test environments and those assigned to the production environment.
* Changes to the system must be made according to the Change Control Policy.
* When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
* The production data source must be sanitized before use in development or test environment and production/test access controls must comply with production standards.
* Test data and accounts must be removed before a production system becomes active.

### ****Secure Development****

* All software development personnel must receive training in writing secure code for their specific development environment.
* A Secure Software Development Lifecycle Standard must be developed and implemented.
* Access to program source code should be restricted based on principle of least privilege.
* For applications that store or transmit confidential information controls must be implemented to limit output to minimum necessary as defined by the user.
* Any outsourced software development should comply with the Secure Software Development Lifecycle Standard recommendations.
* Modifications to externally developed software packages must be limited to necessary changes and all changes should be strictly controlled.

### System Acceptance

* Acceptance criteria must be provided by the application owner and should specify:
  + The operational and functional requirements of the application.
  + Performance and capacity requirements.
* All acceptance criteria must be satisfied before any application can move into a production environment.

Definitions

See Appendix A: Definitions

References

* ISO 27002: 7, 9, 12, 14
* NIST CSF: PR.AT, PR.DS, PR.IP

Waivers

Waivers from certain policy provisions may be sought following the (District/Organization) Waiver Process.

Enforcement

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

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Modified Date | Approved Date | Approved By | Reason/Comments |
| 1.0.0 | February 2018 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |