System Development and Procurement Policy, version 1.0.0

Status: ☐ Working Draft ☒ Approved ☐ Adopted
Document Owner: Information Security Committee
Last Review Date: August 2020

System Development and Procurement Policy

Purpose

The purpose of the Taqnyat System Development and Procurement Policy is to establish the rules for evaluating, developing, and/or deploying **Information Resources**.

Audience

The System Development and Procurement Policy applies to individuals who participate in the procurement, development, or operation of any Taqnyat **Information Resource**.

Contents

Policy

General

- Applications created or deployed inside the Taqnyat IT environment must follow a standardized application lifecycle established by management.
- Applications should be actively maintained and require periodic updates to address **vulnerabilities**. If an application is no longer supported by the vendor, developer, or another party, it must be evaluated for replacement.
- At the onset of the acquisition or design planning phase security requirements must be identified and provided in the System Security Requirements Form.
- All software developed must be based on the Secure Software Development Lifecycle Standard.
- Development, testing, and operational environments must be separated.
- Separation of duties and access controls 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 Taqnyat Change Control Policy.
- 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 Software 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, security 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.
- All newly developed software and updates or revisions to existing software must be fully tested and accepted prior to deployment to the production environment.

System Procurement

- Procurement of new hardware and software must be authorized by Information Technology and requested through the company procurement process.
- Information Technology must perform a review of all new hardware or software prior to final purchase commitment to ensure that necessary security controls can be configured.
- All newly procured hardware and software must be fully tested and accepted prior to deployment to the production environment.
- Deployment of new hardware and software to the production environment must be in accordance with the Change Control Policy.

System Acceptance

- Acceptance criteria must be provided by the **application\resource owner** and should specify:
    - operational and functional requirements of the application,
    - performance and capacity requirements,
    - data classification,
    - hardware specifications, if applicable.
- All acceptance criteria must be satisfied before any system or 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
- Change Control Policy
- Secure Software Development Lifecycle Standard
- System Security Requirements Form

Waivers

Waivers from certain policy provisions may be sought following the Taqnyat 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	Jan- 2023		CISO	Document Origination

NEED HELP?

FRSecure is a full-service information security consultancy.

If you need assistance with anything in this resource, please don't hesitate to reach out to us.

CONTACT US

(877) 767 – 1891 | 6550 York Ave S #500, Edina, MN 55435

For security emergencies, or quotes on services **reach out to us here**.

More resources