# Information Security Process - System, Service, and Software Procurement

## Policy Statement

This Process supports the {Company} Information Security & Privacy Program, and outlines the actions required for procurement of information systems, services, and software for use within {Company}.  The parent Controls for this process are defined in the Standard - System & Service Acquisition.

## Applicability

Compliance with the procedures outlined in this document is mandatory for all {Company} employees, contractors, vendors, and guests.

## Process

Employee fills out the PO Request Form (available from finance@) AND the Security Review Request Form available at: {Insert link here}.

Includes:

* Software/System/Service Provider
* Cost (per license or total, if enterprise or singular product)
* Number of licenses/units needed (as applicable)
* {Company} Owner (primary contact that will be responsible for set-up, etc.)
* {Company} Team (primary user group)
* Is this/will this service be used by other {Company} teams?
* Purchase Approver (Director or higher) - forward written approval to helpdesk@
* Business Use Case
* What types of information will be stored with the service/system/software?
* Where does that data come from?
* Is this software/system integrated into our software offerings?

The completed Security Review Request Form will be sent to infosec@ for review and approval, as appropriate. The Security Team will coordinate with the IT Team for review of Technical Need/Approval.

***\*\* For license requests of existing services/software:***

IT Performs a Review of Technical Need/Approval: (within 2 business days)

        Includes:

* Role-based appropriateness/need is addressed
* Business usage need is addressed
* Written approval for license expense received (Director level or higher)

IT approves or denies the request.

* If denied, the employee is notified of decision and reason.
* If approved, IT assists employee in set-up.

***\*\* For requests of New services/systems/software, OR Contract/Configuration Extensions of existing services/systems/software:***

IT Performs a Review of Technical Compatibility: (within 3 business days)

        Includes:

* Current system LDAP/SSO connection capability
* Unique/Specific need is addressed
* Company-wide usage opportunity

IT approves or denies the request.

* If denied, the employee is notified of decision and reason.
* If approved, IT forwards request and review details to the Security Team.

Security performs a Review of Security/Privacy Controls in place, and compatibility with federal customer guidelines: (contacts vendor within 2 business days of receipt, reviews responses within 3 business days of receipt from vendor)

Includes:

* Data types
* Data storage location
* Current certifications/accreditations
* Privacy, terms of service, and usage policies
* Transfer and storage encryption and security controls
* Patch and maintenance obligations and schedules
* Backup schedules
* Data retention policies/schedules
* Data loss/leakage policies and responsibilities
* Security functions
* Security strength
* Security assurance
* Security documentation

Security approves or denies the request.

* If denied, the employee is notified of decision and reason.
* If approved, Security forwards request and review summaries to finance@.

Contracts Administration & Finance review Contract and Pricing: (within 3 business days of receipt)

Includes:

* Pricing structure & payment terms
* General Terms and Conditions
* Legal obligations of both parties
* Contract length, extension, and termination procedures
* Support obligations
* Availability obligations
* Data/Intellectual property rights

Finance and Contracts Administration approve or deny the request.

* If denied, the employee is notified of decision and reason.
* If approved, Employee and IT are notified to begin Integration and setup for the service.

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.0 |
| Date Modified | 30 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |