Utah Department of Human Services

Application and Software Request, Review and Approval

Application Name:

Date:
Month Day, Year

Instructions and additional information
This form should be completed prior to any new purchase for a solution (software, application, or hardware) that does not appear on the DTS ARB approved list.

All ARB requests should be submitted by an individual authorized by the DOBI IT Governance Group. DOBI IT Governance Groups should discuss all possible ARB requests during IT Governance meetings and receive approval from the IT Governance Group to submit an ARB Request prior to submitting the ARB Request.

Step 1: Receive approval from DOBI IT Governance Group to submit ARB Request.
Step 2: DOBI designee completes Part 1 of the ARB Request.
Step 3: DOBI designee coordinate with designated DTS IT Manager to complete Part 2 of the ARB Request.
Step 4: DOBI Security Officer and DOBI Privacy Officer complete Part 3 of the ARB Request.
Step 5: ARB Group (comprised of DTS/DHS staff) reviews completed ARB Request and will perform one of the following actions:
   1. Approve request and send back to DOBI IT Governance Group. Step 6 follows this.
   2. Denies request and notified DOBI IT Governance Group with reasoning. No further steps occur after this.
   3. Forward request to DTS ARB Group for review if the request is for a system that requires a higher level of approval. DTS ARB will either approve the request, with Step 6 following, or deny the request, at which time the DOBI IT Governance Group will be notified with the reasoning.
Step 6: DOBI IT Governance Group verifies all required policies, procedures and processes are implemented.
Step 7: DOBI IT Governance Group authorizes requested system to go into production.
Part 1: General Information and Business Case

Part 1 is to be filled out by the DHS employee or business representative who is requesting the system being reviewed. The proposed system should already have been discussed in your DOBI IT Governance group and reviewed to ensure it will meet the business use case. This document and process is meant to ensure the proposed system meets administrative, privacy and security requirements. It is recommended that you complete this section with the assistance of your DTS IT Manager.

System Owner:

Vendor/System Name: Enter System Name

Vendor/System Website:

Executive Summary: Enter a summary of what the system you are requesting is and why you are request it?

Problem Statement: What problem are you looking to solve with this system?

Current Solution: How are you currently completing this business function without this system?

Cost Estimate of the Project: How much do you estimate the system will cost to implement?

Funding Source for the Project: What is your funding source for the system?

Who is the designated project manager responsible for the planning and implementation of this system? Name of Project Manager

Please obtain approval from the DHS-DTS IT Director if you want to use a DTS project manager to fill this role.

Data Classification (identify the types of data that will or may be stored, processes and/or transmitted in this system):

☐ Public:
☐ Private/Personal Identifiable Information (PII)
☐ Restricted
☐ Federally Governed
  ○ ☐ PCI
  ○ ☐ HIPAA

This data classification is for the assessment privacy and security requirements only. Your DOBI is responsible for using alternative processes for reviewing and classification data in this system in regards to data retention and GRAMA requirements.
Utah Department of Human Services
Application and Software Review Request

- ☐ FTI
- ☐ SAMSHA
- ☐ Other: [Click here to enter text.]

System Categorization:
Impact is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

☐ Very Low
☐ Low
☐ Moderate
☐ High
☐ Very High

Number of end users and privileged users: [In the table below, provide the approximate number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]

<table>
<thead>
<tr>
<th>Number of Users</th>
<th>Number of Administrators/Privileged Users</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Super Administrator</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
</tr>
</tbody>
</table>

What amount of funding or hours are being allocated to provide Help Desk/User Support for the System: [Describe funding and/or man hours that will be allocated]

- DTS does not provide Help Desk supports for internal DHS information systems without a separate agreement. The requesting DOBI is responsible for providing help desk support to system users. Examples of help desk duties the DOBI should consider that need to be provided are:
  - Serve as the first contact with customers who need technical assistance via the phone or email,
  - Perform troubleshooting using different diagnostic techniques,
  - Provide quick resolution and excellent customer service to system users,
  - Redirect unresolved issues to the next level of support personnel,
  - Provide needed information on IT products or services,
  - Keep record of problems and their resolution
  - Provide feedback on processes and make recommendations on areas to improve
  - Maintain technical documentation and service catalog on installation of software, configuration of hardware and problem troubleshooting.
Will the Division provide users with training on how to appropriately use the System in relation to regulatory or other requirements: Describe what training will be provided

Is the System Section 508 compliant (ADA): ☐ Yes ☐ No

Divisions are responsible for having at least the minimum appropriate policies, procedures and processes in place to ensure all systems are properly implemented, managed and administered. Your D/I/O IT Governance group is responsible for authorizing this system to go into production once all required policies, procedures and processes listed below implemented.

- All systems must have a designated System Owner that is responsible for ensuring all of the following requirements are met.
  - A documented policy that outlines appropriate use for this system.
  - A documented process for adding/removing/changing users and roles. The process should, at a minimum:
    - A documented process for reviewing user access to ensure no unauthorized user or data access occurs. Reviews should be completed at least quarterly.
    - A process to ensure users are properly using the system as intended and in accordance with the ARB approved usage.
    - A process to ensures users only enter authorized data into the system.
    - A process for notifying DTS Security and/or DHS Security of any security or privacy incidents involving this system.
Part 2: DTS IT Implications
Part 2 is to be completed by the division DTS IT Manager.

- Will this application connect to the state network? ☐ Yes ☐ No
  If yes, explain:

- Does this system interface with any other system(s)? ☐ Yes ☐ No
  If yes, what and why:

- Is DTS Helpdesk/Desktop Administration/Management needed?: ☐ Yes ☐ No
  Explain:

- Is DTS Network Support/Administration needed?: ☐ Yes ☐ No
  If yes, explain:

- Is DTS Developer Support/Administration needed?: ☐ Yes ☐ No
  If yes, explain:

- Is DTS Hosting Supporting/Administration needed?: ☐ Yes ☐ No
  If yes, explain:

- What Authentication Method will be used?
  ☐ UtahID
  ☐ SAML
  ☐ Active Directory:
  ☐ Active Directory Federated Services (ADFS)
  ☐ Other: Enter Explanation Here

System Environment: Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices.

System Classification:

In order to sustain and/or recover agency functions during a time of crisis, it is imperative to understand which functions are critical to each agency’s ability to provide services. Priorities must be viewed in a new light in the context of Continuity of Operations. Each function and application an agency performs must be identified and then evaluated in terms of recovery priority.
☐ Tier I—Absolutely critical function with must be restored within 24-48 hours (Agency determined).

☐ Tier II—Essential function that must be restored within 7-28 days (Agency determined).

☐ Tier III—Non-essential function to immediate recovery and Continuity of Operations efforts will be restored as resources permit. 30+ days

☐ Not Applicable—A system this is not hosted or managed by DTS. Recovery time is governed by the contract with the vendor and the vendor is responsible for ensuring recovery/uptime requirements are met.

When Part 1 and 2 are completed, send the form in word format to the DTS IT Director and the DHS Security Officer. The currently contact information for those roles are:
Tricia Cox: tcox@utah.gov
Chris Bramwell: cbramwell@utah.gov

Part 3: Security and Privacy Requirements Review
Part 3 is to be completed by the DOBI designated Security and/or Privacy Officer in coordination with the DTS Campus B Security Officer.

(Note: The source of the requirements reviewed below is NIST Special Publication 800-171, dated December 2016. The requirements being assessed are based on Moderate Impact for Confidentiality as defined in Section 1).

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.
Access Controls Review

1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

2. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

3. Employ the principle of least privilege, including for specific security functions and privileged accounts.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

4. Limit unsuccessful logon attempts.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.
5. Provide privacy and security notices consistent with applicable State of Utah rules and applicable compliance requirements.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

6. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

7. Terminate (automatically) a user session after a defined condition.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.
Awareness and Training

8. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

9. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

Audit and Accountability

10. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.
11. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

12. Review logged events.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

13. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

Identification and Authentication

14. Identify system users, processes acting on behalf of users, and devices.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

15. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☐ Implemented      ☐ Planned to be Implemented      ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

16. Enforce a minimum password complexity and change of characters when new passwords are created.

☐ Implemented      ☐ Planned to be Implemented      ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

17. Store and transmit only cryptographically-protected passwords.

☐ Implemented      ☐ Planned to be Implemented      ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.
Incident Response

18. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

19. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

System and Communications Protection

20. Implement cryptographic mechanisms to prevent unauthorized disclosure of confidential data during transmission unless otherwise protected by alternative physical safeguards.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.
21. Implement cryptographic mechanisms to prevent unauthorized disclosure of confidential data unless at rest unless otherwise protected by alternative physical safeguards.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

Data Storage Location

22. All data is stored, processed, or transmitted only in data centers and/or systems located within the United States.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.

Contract and Agreements

23. Contracts and/or agreements are in place that stipulate that required security and compliance requirements will be implemented and maintained.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable
Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.
Appropriate parties have or will be notified of their role and responsibly regarding the planning, implementing and managing of all security and compliance requirements outlined in contracts and/or agreements.

☐ Implemented  ☐ Planned to be Implemented  ☐ Not Applicable

Provided Current implementation or planned implementation details in text box below. If “Not Applicable,” provide rationale in text box below.
System Review Results:

Does this system meet all baseline DHS security requirements?

- Yes
- No

Is this system approved by DHS Security for review by DTS?

- Yes
- No

Scope of system approval:

- Any changes in system use that are outside of the approved scope below will require a new security review. It is the system owner responsibility to initiate a new security review with the DHS Security Officer.
- DOBI is required to ensure users of the proposed system are aware that they must notify either the designated division Privacy Officer, DHS Security Officer, or DTS Security in the event of a suspected privacy or security incident?
- DOBI is required to ensure required agreements are in place to ensure that all users of the system are required to maintain the confidentiality, integrity and availability of data stored in the system according to regulatory or DOBI defined requirements.
- DOBI is required to allocate resources and support to ensure all privacy, security, compliance, system management, administration and helpdesk requirement are implemented prior to any DOBI data entering the system and through the entire lifecycle of the system.
- DOBI Privacy and Security Officers are required review the privacy and security controls for this system at least annually to ensure system meets any/all applicable privacy, security and compliance requirements.
## Signatures

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Owner Signature</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency Privacy Officer Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency Privacy Officer Signature</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DTS Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DTS Security Signature</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOBI Director</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOBI Director Signature</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>