



utah department of  
human services

## Utah Department of Human Services

### Application and Software Review Request

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.

---

### 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. 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 to you estimate the system will cost to implement?

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

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

**Will the Division provide users with training on how to appropriately use the System in relation to regulatory requirements:** Describe what training will be provided

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

**Who in your D/I/O is responsible for creating policy/procedure to outline appropriate use for users of this system?** Name of individual

**Who in your D/I/O will be acting as system administrator for this system?** Name of individual

The system administrator is responsible for at least the following actions:

- Proper adding/removing/changing of all users and roles.
- Reviewing user access to ensure no unauthorized user or data access occurs.
- Ensures users, in conjunction with system owner, are properly using the system as intended and in accordance with the ARB approved usage.
- Ensures users, in conjunction with system owner, only enter authorized data into

the system.

- Notifying DTS Security and/or DHS Security of any security or privacy incidents.

## Part 2: DTS IT Implications

Part 2 is to be completed by the division DTS IT Manager.

- 1) Will this application connect to the state network?  Yes  No  
If yes, explain:
- 2) Does this system interface with any other system(s)?  Yes  No  
If yes, what and why:
- 3) Is a project manager needed to implements this system?  Yes  No
- 4) Is DTS Helpdesk/Desktop Administration/Management needed?:  Yes  No  
Explain:
- 5) Is DTS Network Support/Administration needed?:  Yes  No  
If yes, explain:
- 6) Is DTS Developer Support/Administration needed?:  Yes  No  
If yes, explain:
- 7) Is DTS Hosting Supporting/Administration needed?:  Yes  No  
If yes, explain:
- 8) What Authentication Method will be used?
  - Utah Master Directory (UMD)
  - SAML
  - Active Directory:
  - Active Directory Federated Services (ADFS)
  - Other: Explain Enter Text HERE

## 9) Technology Summary: Describe the technical architecture of the System

When Part 1 and 2 are completed, send the form in word format to the Campus B DTS IT Director and the DHS Security Officer. The currently contact information for those roles are:

Tricia Cox:

Chris Bramwell: [cbramwell@utah.gov](mailto:cbramwell@utah.gov)

### Part 3: Security Review

Part 3 is to be completed by the DHS Security Officer in coordination with the DTS Campus B Security Officer.

#### 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.

**Data Classification:** See Appendix A for detailed data classification definitions.

**Public:**

**Private:**

- PII

**Restricted**

**Federally Governed**

- PCI
- HIPAA
- FTI

**SAMSHA**

**Other:**

#### Impact 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. See Appendix A for detailed definitions of Impact Categorizations.

Very Low

- Low
- Moderate
- High
- Very High

**R1 - Required** Is there an appropriate authentication mechanism for this system and does each user have a unique identifier and password?

Yes

No

Please detail how requirement is being met if answer is yes or detail any mitigating control that may be in place if answer is no:

Do the current controls in place meet the requirement or do mediating controls properly mediate the risk:

Yes

No

Please rate the likelihood of a threat/vulnerability affecting your data:

Low

Medium

High

**R2 – Required** Does the system have audit control mechanisms that can monitor, record and/or examine information system activity for this system?

Yes

No

Please detail how requirement is being met if answer is yes or detail any mitigating control that may be in place if answer is no:

Do the current controls in place meet the requirement or do mediating controls properly mediate the risk:

- Yes
- No

Please rate the likelihood of a threat/vulnerability affecting your data:

- Low
- Medium
- High

**R3 - Required** Is FIPS 140-2 compliant encryption implemented for this system as the safeguard to assure that data is not compromised when stored?

- Yes
- No

Please detail how requirement is being met if answer is yes or detail any mitigating control that may be in place if answer is no:

Do the current controls in place meet the requirement or do mediating controls properly mediate the risk:

- Yes
- No

Please rate the likelihood of a threat/vulnerability affecting your data:

- Low
- Medium
- High

**R4 - Required** Is FIPS 140-2 compliant encryption implemented for this system as the safeguard to assure that data is not compromised when being transmitted from one point to another?

- Yes
- No

Please detail how requirement is being met if answer is yes or detail any mitigating control that may be in place if answer is no:

Do the current controls in place meet the requirement or do mediating controls properly mediate the risk:

- Yes
- No

Please rate the likelihood of a threat/vulnerability affecting your data:

- Low
- Medium
- High

Please rate the impact of a threat/vulnerability affecting your data:

- Low
- Medium
- High

**R5 - Required** Is all data stored in data facilities in the United States?

- Yes
- No

Please detail how requirement is being met if answer is yes or detail any mitigating control that may be in place if answer is no:

Do the current controls in place meet the requirement or do mediating controls properly mediate the risk:

- Yes
- No

Please rate the likelihood of a threat/vulnerability affecting your data:

- Low
- Medium
- High

**R6 - Required** Does the vendor provide a contract that stipulates the system in question will maintain required baseline security controls?

Yes

No

Please detail how requirement is being met if answer is yes or detail any mitigating control that may be in place if answer is no:

Do the current controls in place meet the requirement or do mediating controls properly mediate the risk:

Yes

No

Please rate the likelihood of a threat/vulnerability affecting your data:

Low

Medium

High

**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 by DHS Security:**

- 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.
- Specific Features or Versions that are not approved for use:

**Signatures**

Agency Reviewers Name: _____
Agency Reviewers Signature: _____
DTS Security Name: _____
DTS Security Signature: _____
System Owner Name: _____
System Owner Signature: _____