



## MODEL PLAN EXTERNAL AGENCY BUSINESS SYSTEM

Department of Financial Services  
Division of Accounting and Auditing  
Bureau of Auditing

## ACRONYMS & DEFINITIONS

### **Access Control Custodian**

An individual responsible for assigning and managing user permissions for the external business system. This person must be independent of Accounts Payable and ideally not be a system user to maintain proper internal control.

### **Background Checks**

Screenings conducted on contractor employees to verify identity, criminal history, or other relevant factors that support safe, secure participation in operating or maintaining the external business system.

### **Batch Control Totals**

A comparison of record counts and control totals before and after processing both files.

### **Batch File**

A file containing transactions for submission to the State's Accounting System.

### **Business Rules (User Access)**

Documented agency policies defining who may access specific system data and functions, ensuring proper separation of duties and alignment with user roles and responsibilities.

### **Cloud Provider**

A third-party hosting service responsible for storing, managing, and operating the external business system and its data when not hosted internally.

### **Confidential Data**

Information protected from unauthorized access that may appear within inquiry-only views in the external business system.

### **Contractor**

An external entity hired to operate or maintain the agency's external business system, potentially including hosting, support, monitoring, and administrative roles.

### **Disaster Recovery**

Processes and controls ensuring the external business system can be restored and made operational after a disruptive event.

### **External Business System (EBS)**

Any technology platform, application, or database that is owned, managed, and operated by a contractor to perform the agency's business activities. These systems support functions such as case management, financial processing, reporting, workflow

automation, and data management. Access is restricted to authorized agency staff, and the system operates within the agency's internal IT controls, security standards, and governance framework.

### **Inquiry Access**

A restricted user access level permitting employees to view system data—including confidential data—without adding, editing, or deleting information.

### **Separation of Duties**

Internal control preventative requiring different individuals to perform creation, approval, authorization, and recording activities.

### **Statements on Standards for Attestation Engagement (SSAE) 18 Audit**

A standardized, independent audit performed by Certified Public Accountants under AICPA guidelines to assess whether a service provider, such as a cloud host or contractor, has effective internal controls related to security, data integrity, and system operations.

### **User Permissions**

System access rights assigned to users defining what data they can view and what functions they can perform.

### **User Roles and Responsibilities**

Defined duties for each system user that determine their appropriate level of access within the external business system.

### **Workflow**

System-supported transactional routing that enforces proper separation of duties for authorization, , receipt verification, and payment recording.

## **PURPOSE**

Agencies using External Business Systems (EBS) to originate, route, or approve transactions before submission to the State's accounting system must document internal controls ensuring authenticity, authorization, completeness, accuracy, and secure handling of financial data.

This Model Plan was developed as a tool to help agencies develop an agency specific plan for their existing external business system, verifying all required internal controls are addressed.

## **SYSTEM OVERVIEW**

Agencies must provide a clear, accurate description of the external business system as it operates today to originate, route, or approve transactions prior to submission to the State's accounting system.

## SYSTEM INFORMATION

System Name:

Acronym:

**Business Owner:**

Name:

Title:

Agency/Division/Office:

**Operational Location:**

Name:

Title:

Agency/Division/Office:

**System Owner:**

Name:

Title:

Agency/Division/Office:

## SYSTEM OVERSIGHT AND CONTROLS

1. Is your External Agency business system maintained and operated by a contractor?

☐ Yes

☐ No

If yes, does the contractor's employees undergo background checks and are routinely monitored?

**Describe whether the contractor's employees undergo background checks and are routinely monitored, including the types of screenings conducted, the frequency of ongoing monitoring, and any controls in place to ensure compliance with State requirements.**

2. Does a cloud provider host your external business system and related data with the contractor who makes it available to the agency for program operations and payments?

**Describe whether a cloud provider hosts the external business system and related data used by the contractor, and whether the contractor makes this system and data available to the agency to support program operations and payment processing.**

3. Does the contractor and cloud provider receive a SSAE 18 audit on internal controls and are the results provided to the agency for review and follow-up?

**Describe whether the contractor and the cloud provider undergo an SSAE 18 audit of their internal controls, and whether the resulting audit reports are provided to the agency for review and any necessary follow-up actions.**

4. From the audit, if internal control weaknesses are noted, has the agency assessed the risk on operations and is there a corrective action plan to bring the controls into compliance?

**Describe whether the agency evaluates any internal control weaknesses identified in the audit, including how risks to operations are assessed and whether a corrective action plan has been established to bring the controls into compliance.**

Note: It is very important as part of the contractual relationship to receive an audit that is comprehensive and covers disaster recovery and continuity of operations.

## USER ACCESS CONTROLS

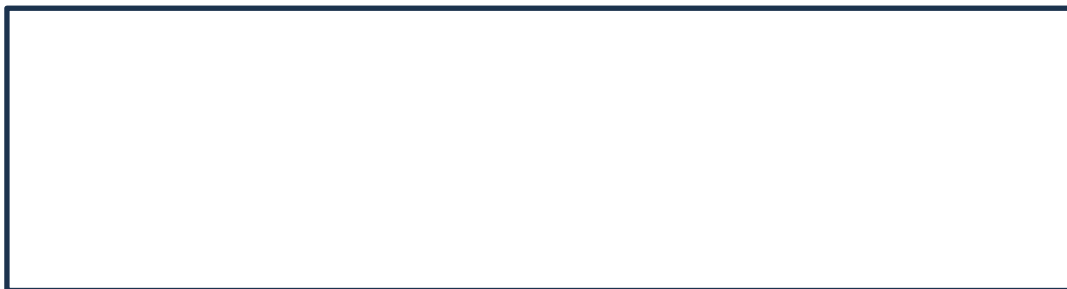
1. Does your Agency maintain up to date business rules that defines user access in the context of separating the receipting, authorizing and financial recording functions?

**Describe whether the agency maintains up-to-date business rules that define user access requirements, including how these rules ensure the proper separation of duties between receipting, authorizing, and financial recording functions.**



2. Are the business rules based on user roles and responsibilities with limits on the types of information users can access, and supported with up-to-date position descriptions?

**Describe whether the agency's business rules are established based on user roles and responsibilities, including limits on the types of information users are permitted to access, and whether these rules are supported by up-to-date position descriptions that clearly outline assigned duties and access requirements.**



3. When changes to user access occur, do the changes include a sound basis within the context of internal control, and are the changes documented and supported?

**Describe whether changes to user access are made based on a sound internal control rationale, including how the agency ensures that each change is properly justified, documented, and supported in accordance with established access management and oversight procedures.**



4. For users who have inquiry access only, does the access include confidential data and is their access included in the business rules and position description?

**Describe whether users with inquiry-only access can view confidential data, and whether this level of access is defined within the agency's business rules and reflected in the users' position descriptions, including how such access is justified and monitored.**



5. Does the external business system have workflow to support the separation of transaction authorization, receipt of goods and services, and recording of payment?

**Describe whether the external business system includes workflow functionality that supports the separation of duties for key processes, including transaction authorization, receipt and verification of goods and services, and the recording of payments, and explain how the workflow ensures proper internal control and oversight.**



6. Does someone other than those involved with or responsible for accounts payable control and assign user permissions to the agency business system? The access control custodian should not be a user.

Note: A best practice is to assign someone not in accounts payable or the creation of batch files to control user permissions.

**Describe whether user permissions for the agency's business system are controlled and assigned by an individual who is independent of the accounts payable function, ensuring that the access control custodian is not a system user, and does not participate in accounts payable activities.**



#### TRANSFERRING BATCH FILES FOR PROCESSING

1. Is the process for uploading accounts payable batch files to the accounting system limited to only employees who need it for their assigned duties?

Note: This should be an IT function and not accounts payable.

**Describe whether the process for uploading accounts payable batch files is restricted to employees who require this capability for their assigned duties, including how access is limited, monitored, and controlled to ensure proper separation of duties and compliance with internal controls.**



2. Is the batch file reviewed and signed off on Accounts Payable personnel prior to processing?

**Describe whether the batch file is reviewed and formally signed off by Accounts Payable personnel prior to processing, including the steps taken to verify accuracy, completeness, and compliance before the file is approved for submission.**

A large, empty rectangular box with a dark blue border, intended for the user to provide a detailed response to the question above.

3. Are there controls in place to prevent the changing of data once the batch file has been created by the external business system?

**Describe whether controls are in place to prevent data from being altered after the batch file has been created by the external business system, including any system-enforced restrictions, audit trails, or monitoring mechanisms that ensure the integrity of the file before processing.**

A large, empty rectangular box with a dark blue border, intended for the user to provide a detailed response to the question above.