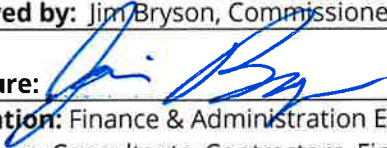


# POLICY

<b>Approved by:</b> Jim Bryson, Commissioner	<b>Policy Number:</b> 41
<b>Signature:</b> 	<b>Supersedes:</b> N/A
<b>Application:</b> Finance & Administration Employees, Volunteers, Consultants, Contractors, Finance & Administration Service Recipients, and Finance & Administration Grant Sub-recipients	<b>Effective Date:</b> September 01, 2023
<b>Authority:</b>	<b>Rule:</b>

**Subject:**

**REPORTING A GRANT SUBRECIPIENT'S BREACH OF PERSONALLY IDENTIFIABLE INFORMATION**

**I. Statement of Purpose.**

The purpose of this policy is to standardize the process for Tennessee Department of Finance and Administration ("F & A") staff response and reporting of an incident or breach of personally identifiable information (PII) by a grant subrecipient organization. This purpose will be met by consistent process for responding to subrecipient data breaches; meeting federal reporting requirements; and meeting records management requirements.

**II. Definitions.**

**"Breach"** means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for other than authorized purposes.

**"Incident"** means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

**"Personally identifiable information (PII)"** means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifiable information that is linked or linkable to a specific individual.

**III. Scope of Policy.**

This policy applies to F & A in its capacity as a state authorizing grant agency and does not in any way alter, conflict with, or undermine any state or federal breach reporting requirements applicable to F & A in its capacity as an executive branch agency of the State of Tennessee.

# F & A Policy:

## REPORTING A GRANT SUBRECIPIENT'S BREACH OF PERSONALLY IDENTIFIABLE INFORMATION

**Policy Number: 41**

Revised:  
September 01, 2023

### IV. Responding to a Data Breach and Reporting.

When notified of an incident or breach within a grant subrecipient organization, the applicable grant staff shall review the subrecipient's active and expired contracts to determine whether additional information must be collected and whether federal reporting is required.

1. If federal reporting is required:
  - (A) US Department of Justice Awards. F & A staff shall submit the report to the DOJ Senior Policy Advisor (SPA) within 24 hours of receipt of notice of an incident or imminent breach from a subrecipient.
  - (B) Other Federal Awards. F & A staff shall submit the report to appropriate federal grant manager in the time and manner designated by the applicable grant conditions and federal requirements.
2. If the grant subrecipient only receives state funding, F&A staff shall promptly comply with applicable state reporting law and policy upon receipt of an incident or breach.
3. F & A staff shall collect a copy of the subrecipient's breach policy as well as all steps taken by the subrecipient to resolve the incident/breach and to notify individuals potentially impacted by the incident/breach.
4. F & A may require the subrecipient to submit a Corrective Action Plan (CAP) if it is determined that there is a weakness in the breach policy, practices, other internal controls. F & A staff shall respond to subrecipient CAPs within 30 business days of receipt.

### V. Records Management.

F & A shall place all breach related documentation, including correspondence, notice documents, CAPS, and all other documents in the respective subrecipient program file. All breach-related documentation shall be retained in accordance with the Records Disposition Authorization for the applicable grant. If the impacted organization's grant includes federal fund sources, F & A shall also save all federal and subrecipient correspondence to the applicable federal award notebooks.