GovRAMP Box portal evidence submission.

* Include **date/time stamp** on all documents and screenshots where applicable.
* Description – Include a narrative on how the artifact supports the control requirement(s).
  + For example, AC-2(j)- description and evidence/screenshot supporting a quarterly review for privileged accounts access and an example of an annual review for all other users (non-privileged).
  + Attach as many screenshots needed to support how the control is being met.
  + The same evidence can be uploaded for multiple controls where applicable.

Other forms of documents can be uploaded to the folder as in policies, procedures, scans, etc.

|  |  |
| --- | --- |
| Control ID: AC-02 |  |
| Description:   1. Define and document the types of accounts allowed and specifically prohibited for use within the system; | *Control Implementation Statement; evidence references* |
| 1. Assign account managers; |  |
| 1. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; |  |
| 1. Specify:   1. Authorized users of the system;  2. Group and role membership; and  3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; |  |
| 1. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; |  |
| 1. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; |  |
| 1. Monitor the use of accounts; |  |
| 1. Notify account managers and [Assignment: organization-defined personnel or roles] within:   1. [Assignment: organization-defined time period] when accounts are no longer required;  2. [Assignment: organization-defined time period] when users are terminated or transferred; and  3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; |  |
| 1. Authorize access to the system based on:   1. A valid access authorization;  2. Intended system usage; and  3. [Assignment: organization-defined attributes (as required)]; |  |
| 1. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; |  |
| 1. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and |  |
| 1. Align account management processes with personnel termination and transfer processes. |  |