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: SI-03 |  |
| Description:  a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; | *Control Implementation Statement; evidence references* |
| b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; |  |
| c. Configure malicious code protection mechanisms to:  1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and  2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and |  |
| d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system. |  |