

# Government Entity Security Policy Agreement

The Service Provider has adopted the following *Online Account Security Agreement*, which outlines your responsibilities for securing and using an official username and password for access to secure online applications. Use of a Service Provider secure online application requires your acceptance of all the policy terms and conditions stated below:

- All persons requesting access to an application or service must complete necessary training.
- You must not share your account with other individuals for any reason. Your online account is to be used only by you for official business purposes. The sharing of passwords exposes the authorized user to responsibility for all actions taken with their login credentials. As an authorized user, you will not cause or permit any other person to access the application by use of your login credentials.
- **USERS FOUND SHARING THEIR ACCOUNT WITH ANOTHER INDIVIDUAL WILL HAVE THEIR ACCOUNT DEACTIVATED IMMEDIATELY.**
- If your login credentials are compromised, or if you believe a user other than yourself has accessed your account—you are responsible for immediately contacting your Entity Project Manager or the Service Provider at 303-534-3468.
- You are responsible for notifying your Entity Project Manager with requests for additional access, or if you no longer need access to the Service Provider secure digital solutions. Contact your Entity Project Manager with any questions regarding password changes.

Organization Name:	
Full Name of New User:	
Title:	
Entity Project Manager:	
Work Mailing Address:	
Work Telephone:	
Work Email:	

Access is requested to the following digital solution(s):

- |  |  |
|--|--|
| <input type="checkbox"/> Content Management System (Website) | <input type="checkbox"/> Prompt Pay  |
| <input type="checkbox"/> Engagement Builder (AccessGov)      | <input type="checkbox"/> TPE/NIC   |
| <input type="checkbox"/> PayPort                             | <input type="checkbox"/> Other (MIIDB, DRIVES, EUDL, Bulk Records, etc...) |

List the primary URL used by your organization for this digital solution:

--

I have read the above and agree to abide by its provisions. I understand that violation of the provisions stated in the policy may cause suspension or revocation of online access and related privileges.

---

**Signature**

**Date**

I certify that the user is authorized to access the applications or site administrative interfaces listed on this document. I understand that I am responsible for notifying the Service Provider of any future changes or termination of user permissions.

---

**Authorization Signature**

**Date**

**(Entity Project Manager or Authorized Agent must approve all users)**

