

Digital Autopen for Federal Register Documents Playbook

Template - User Agreement

**March 2023**

**FINAL**

**Federal Chief Information Security Officer Council**

**Identity, Credential, and Access Management Subcommittee**

**Delegated Digital Signature Working Group**

Name of User:

The agency employee must sign this cardholder responsibility agreement before issuing a digital autopen certificate ("the certificate"). The following documents govern the certificate:

1. Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors;
2. Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors;
3. X.509 Certificate Policy for the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework, and
4. National Institute of Standards and Technology (NIST) Special Publication 800-157, Guidelines for Derived PIV Credentials.

As a digital autopen certificate holder, I agree to the following:

1. I will use the certificate for official purposes only. I will digitally sign *Federal Register* documents only after the [authorizing sponsor] has approved the *Federal Register* document and after the [authorizing sponsor] has directed the use of the digital autopen.
2. I will always maintain control of the certificate and not allow anyone to use it for any unauthorized purpose. When not performing duties at my work site, I shall store the certificate in a secure (i.e., locked) location.
3. I will ensure the proper records are created, followed, and archive when the [authorizing sponsor] approves use of the digital autopen certificate in my control.
4. I will not move or copy this certificate to another device and will only use this credential on an agency issued device.
5. I will create a password or PIN that is not easily guessable or individually identifiable and protect the password/PIN by not giving it to others or making it easily accessible.
6. I will always protect this certificate from loss, unauthorized disclosure, or suspicion of compromise.
7. I will report changes to the [head of the office with delegated authority] to my employee status (e.g., Federal employee to contractor, etc.); my role status (e.g., emergency response official, etc.); a change in my name; if this certificate is nearing expiration, or other changes that impact the integrity of the digital autopen certificate.
8. I will report a compromised, lost, or stolen certificate to [Insert Agency Security Information], so they can immediately revoke it.
9. I understand that I may be subject to administrative action if I misuse the certificate or if it is compromised, lost, or stolen through my non-compliance with these requirements.
10. I will surrender the certificate to the appropriate authority when my employment or association with [Agency] is terminated; or upon request by the appropriate authority.

[Agency] Rights and Responsibilities:

1. [Agency] will not disclose certificate keys issued from the Certificate Authority (CA), except with the consent of the certificate holder or as required by law.
2. [Agency] reserves the right to refuse to issue certificates to any person, and such decision may be made by [Agency] without notice and at its sole discretion. In addition, [Agency] may revoke any certificate at any time without notice.

I acknowledge that I have read and understood the above and agree to the terms.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Employee Signature |  | Printed Name |  | Date |