



Cross-Media Electronic Reporting Regulation (CROMERR)

Electronic Signature Agreement Guide

| | |
|--|----|
| Electronic Signature Agreement Requirements..... | 2 |
| Electronic Signature Agreement Example..... | 4 |
| Electronic Signature Agreement Template | 6 |
| Subscriber Agreement Example | 8 |
| Subscriber Agreement Template | 10 |



Electronic Signature Agreement Requirements

Attached is an example of electronic signature agreement language that may be used, in part, to satisfy the electronic signature agreement or subscriber agreement requirement of 40 C.F.R. § 3.2000(b)(5)(v). Applicants need to include a copy of the electronic signature agreement in their CROMERR application.

CROMERR requires that users sign an electronic signature agreement, or ESA, normally as part of the registration process. This agreement must include language that obligates the registrant to protect the electronic signature device (or signature credential) from compromise, and to immediately report any evidence of compromise to the system administrator. The agreement must also include a statement that the registrant understands that any electronic signature executed with the electronic signature device is as legally binding as a handwritten signature. ESAs are not needed for reports that do not require an electronic signature.

The ESA can be done electronically, but can also be done on paper with a handwritten signature as described in 3.2000(b)(5)(vii)(C). When done on paper it is called a subscriber agreement. See the box to the right for definitions of electronic signature agreement and subscriber agreement. An ESA is an agreement done online, while a subscriber agreement is done on paper with a handwritten signature. Usually, signatories execute one of these agreements when they register with the system to receive their electronic signature device.

ESAs completed electronically may be signed using the electronic signature device the signatory establishes during the registration process. If this device is not used, the system application must describe how the system ensures that the ESA has been signed by the registrant.

Storing Subscriber Agreements

Systems using the subscriber agreement alternative must store the paper agreements so they are protected from alteration and destruction for as long as there may be any enforcement interest in the signatures executed with the associated electronic signature device, or at least five years after the signature credential has been deactivated.

Note that this item must be addressed only for reports that require an electronic signature, including priority reports, where the system requires a paper electronic signature agreement to be signed by users. This is most commonly used by systems using the CROMERR subscriber agreement alternative under 40 CFR 3.2000(b)(5)(vii)(C). Applications should describe how they plan to store paper electronic signature agreements in a way that protects them from tampering, destruction, and unauthorized access. Typically, program offices store original signed paper subscriber agreements in locked filing cabinets that are only accessible by designated staff.

Key Definitions

An electronic signature agreement is an agreement signed by an individual with respect to an electronic signature device that the individual will use to create his or her electronic signatures requiring such individual to protect the electronic signature device from compromise; to promptly report to the agency or agencies relying on the electronic signatures created any evidence discovered that the device has been compromised; and to be held as legally bound, obligated, or responsible by the electronic signatures created as by a handwritten signature. (See 40 CFR 3.3)

A subscriber agreement is an electronic signature agreement signed by an individual with a handwritten signature. This agreement must be stored until five years after the associated electronic signature device has been deactivated. (See 40 CFR 3.3)



Specific ESA and Subscriber Agreement Requirements

Below is a list of specific items to focus on in electronic signature agreements. The agreement must include the following:

- (1) The signatory agrees to protect their signature device, such as a password, answers to security questions or hardware token, from compromise;
- (2) The signatory agrees to report any evidence of compromise; and
- (3) The signatory understands that the signature they submit electronically with the device carries the same legal force and obligation as a hand written signature.

ESA Best Practices

- Using the ESA to determine the registrant's signing authority: CROMERR requires that systems determine with legal certainty that the individuals who sign submissions to environmental agencies are explicitly authorized to do so, by their management and/or by the agency to which they report. Some ESAs include a signature block for a responsible official from the registrant's authorization for the signatory to sign on behalf of the organization. If the ESA is also used to certify that the signer has the authority to sign on behalf of the organization, a new ESA may need to be submitted each time the authorization changes (e.g., if a company comes under new ownership). For this reason, EPA recommends that ESAs not include signatory authorization in the ESA. Many States find it less burdensome to include authorization in a separate document or use another means to confirm signatory authorization.
- Notarization of paper subscriber agreements: Some approved CROMERR systems require that paper subscriber agreements be notarized. This is not required by CROMERR but can be an effective way to ensure at the time of registration that the registrant is who they claim to be.
- Citing regulations in the ESA: CROMERR does not require that the ESA cite specific laws or regulations under which reporting is required, or law or regulations that govern electronic signatures.

*EPA recommends that you do not include the bolded language below in your ESA: "No document shall satisfy any reporting requirement **or be of any legal effect** until properly received."*

Some ESAs submitted as part of previously approved CROMERR applications included this language. However, EPA has determined that this language may become an impediment to certain enforcement proceedings. EPA may need to conduct enforcement proceeding based on documents that users attempt to submit but might not be properly received. Inaccurate or false submissions may be used in enforcement proceedings even if rejected by the receiving systems. The bolded language above may preclude EPA from using such documents in an enforcement process.



Electronic Signature Agreement Example

U.S. Environmental Protection Agency ELECTRONIC SIGNATURE AGREEMENT

In accepting the electronic signature credential issued by the U.S. Environmental Protection Agency (EPA) to sign electronic documents submitted to EPA's Central Data Exchange (CDX), and as a representative for:

Electronic Signature Holder Company Information

| | |
|-------------------|-----------------------------------|
| Organization Name | (pre-populated w/credential info) |
| Address | (pre-populated) |
| City, State, Zip | (pre-populated) |
| Province | (pre-populated) |
| Country | (pre-populated) |
| Phone Number | (pre-populated) |
| E-mail Address | (pre-populated) |
| Registrant's Name | (pre-populated) |
| CDX User Name | (pre-populated) |

I, _____ Populated from registration _____, (Name of Electronic Signature Holder)

(1) Agree to protect the electronic signature credential, consisting of my Central Data Exchange (CDX) user identification, password and answers to security questions, from use by anyone except me. Specifically, I agree to maintain the secrecy of the password and answers to my security questions; I will not divulge or delegate my user name, password and answers to security questions to any other individual; I will not store my password and answers to security questions in an unprotected location; and I will not allow my password and answers to security questions to be written into computer scripts to achieve automated login;

(2) Agree to contact the U.S. EPA CDX Help Desk at 1-888-890-1995 as soon as possible, but no later than 24



hours, after suspecting or determining that my user name, password and answers to security questions have become lost, stolen or otherwise compromised;

(3) I agree to notify CDX within ten working days if my duties change and I no longer need to interact with the CDX on behalf of my organization. I agree to make this notification by notifying the CDX Technical Support staff at 1-888-890-1995 or helpdesk@epa.gov

(4) Understand that I will be informed through my registered electronic mail (e-mail) address whenever my user identification or password have been modified;

(5) Understand that CDX reports the last date my user identification and password were used immediately after successfully logging into CDX;

(6) Understand and agree that I will be held as legally bound, obligated, and responsible for the use of my electronic signature as I would be using my hand-written signature;

(7) Understand that whenever I electronically sign and submit an electronic document to the CDX, I will receive an e mail at my registered e mail address; This e-mail will inform me that a submission has been made to CDX from my user account and will contain instructions to view information regarding the submission, including my Copy of Record (CoR);

(8) Agree that if I receive an e mail notification for any activity that I do not believe that I performed, I will notify the CDX Help Desk as soon as possible, but no later than 24 hours, after receipt;

(9) Agree to contact the CDX Help Desk if I do not receive an e mail notification within 5 business days for any electronically signed submission using my credentials;

(10) Agree to report, within 24 hours of discovery, any evidence of discrepancy between any electronic document I have signed and submitted and what the CDX has received from me by contacting the CDX or service Help Desk;

(11) Agree to notify the EPA if I cease to represent the regulated entity specified above as signatory of that organization's electronic submissions by contacting the CDX Help Desk as soon as this change in relationship occurs and to sign a surrender certification at that time; and,

(12) Agree to retain a copy of this signed agreement as long as I continue to represent the regulated entity specified above as signatory of the company's electronic submissions.

Name of electronic signature holder: pre-populated from Registration

Transaction ID: pre-populated from 20-5-1

Date: _____



Electronic Signature Agreement Template

Electronic Signature Agreement

In accepting the electronic signature credential issued by [insert State/Commonwealth name] to sign electronic documents submitted to [insert name of reporting system], and as a representative for:

Electronic Signature Holder Company Information

| | |
|-------------------|-----------------------------------|
| Organization Name | (pre-populated w/credential info) |
| Address | (pre-populated) |
| City, State, Zip | (pre-populated) |
| Province | (pre-populated) |
| Country | (pre-populated) |
| Phone Number | (pre-populated) |
| E-mail Address | (pre-populated) |
| Registrant's Name | (pre-populated) |
| CDX User Name | (pre-populated) |

I, Populated from registration ,

(Name of Electronic Signature Holder)

[The following certifications are required]

(1) Agree to protect the electronic signature credential, consisting of my [insert name of reporting system] [insert signature credential type, e.g., username, password and answers to security questions], from use by anyone except me. Specifically, I agree to maintain the secrecy of the [insert signature credential type]; I will not divulge or delegate my [insert signature credential type] to any other individual; I will not store my [insert signature credential type] in an unprotected location; and I will not allow my [insert signature credential type] to be written into computer scripts to achieve automated login;

(2) Agree to contact the [insert name of reporting system] at [insert reporting system phone number] as soon as possible, but no later than 24 hours, after suspecting or determining that my [insert signature credential type] have become lost, stolen or otherwise compromised;



(3) Understand and agree that I will be held as legally bound, obligated, and responsible for the use of my electronic signature as I would be using my hand-written signature;

[The following certifications are optional but recommended]

(4) I agree to notify [insert name of reporting system] within ten working days if my duties change and I no longer need to interact with [insert name of reporting system] on behalf of my organization. I agree to make this notification by notifying [insert name of reporting system] staff at [insert reporting system contact information];

(5) Understand that I will be informed through my registered electronic mail (e-mail) address whenever my user identification or password have been modified;

(7) Understand that whenever I electronically sign and submit an electronic document to [insert name of reporting system], I will receive an e-mail at my registered e-mail address; This e-mail will inform me that a submission has been made to [insert name of reporting system] from my user account and will contain instructions to view information regarding the submission, including my Copy of Record (CoR);

(8) Agree that if I receive an e-mail notification for any activity that I do not believe that I performed, I will notify [insert name of reporting system] as soon as possible, but no later than 24 hours, after receipt;

(9) Agree to contact [insert name of reporting system] if I do not receive an e-mail notification within 5 business days for any electronically signed submission using my credentials;

(10) Agree to report, within 24 hours of discovery, any evidence of discrepancy between any electronic document I have signed and submitted and what [insert name of reporting system] has received from me by contacting [insert name of reporting system];

(11) Agree to notify [insert name of reporting system] if I cease to represent the regulated entity specified above as signatory of that organization's electronic submissions by contacting [insert name of reporting system] as soon as this change in relationship occurs and to sign a surrender certification at that time; and,

(12) Agree to retain a copy of this signed agreement as long as I continue to represent the regulated entity specified above as signatory of the company's electronic submissions.

Name of electronic signature holder:

Date: _____

[Insert mailing address for reporting system]



Subscriber Agreement Example

Electronic Subscriber Agreement

Please complete the following form and mail to:

Florida Department of Environmental Protection Attn:

{Contact.contactName}

2600 Blair Stone Road

{Contact.addressLine2}

Tallahassee, FL 32399

User ID: —
Name: —
Telephone: —
Email: —
Street Address: —
City: —
State: —
Zip Code: —

I,____, the undersigned, am hereby submitting this Subscriber Agreement to the Florida Department of Environmental Protection (FDEP) in application for a Personal Identity Number that shall, along with my username, password and additional personal security information, serve as the Electronic Signature Device and equivalent of my handwritten signature on all electronically submitted reports, documents, applications, files and forms to the FDEP. I hereby:

1. Agree to protect my electronic signature device and security question/answer pairs from compromise and from use by any other party, including anyone who may be acting as my agent;
2. Promptly report (within 24 hours after discovery) to the FDEP any evidence of the loss, theft, or other compromise of this electronic signature device and/or security question/answer pairs;
3. Review and, if necessary, repudiate, any electronic reports, documents,



applications, files and forms that may have been submitted to the FDEP after this loss, theft or compromise;

- 4. Promptly review (within 24 hours after discovery), the acknowledgements (email and onscreen) and copies of submitted documents using this electronic signature device, and;
- 5. Promptly report (within 24 hours after discovery) evidence of discrepancy between any electronically submitted information signed using this electronic signature device and what was received by the FDEP's electronic receiving system.

I understand that I shall be held as legally bound, obligated, and responsible by the electronic signature created using this electronic signature device as by my handwritten signature.

Applicant Signature:____Date: _____

Notarization of Electronic Signature Device and Subscriber Agreement

[Note: Notarization is not required by CROMERR]

In the State of: ____

and the County of: _____

On____before me,_____, (date of signing) (Notary's name)

personally appeared____, personally known to me (or proved to me on the basis of satisfactory evidence) to be the person whose name is subscribed within this instrument and acknowledged to me that he/she executed the same in his/her authorized capacity and that by their affixed signature on this instrument do affirm their lawful execution thereof.

Witness therefore my hand and official seal (Notary Seal)

(Signature of Notary)



Subscriber Agreement Template

Electronic Subscriber Agreement

Please complete the following form and mail to:

[*insert State/Commonwealth name*]

Attn: [*insert contact name*]

[*insert contact address*]

User ID: —
Name: —
Telephone: —
Email: —
Street Address: —
City: —
State: —
Zip Code: —

I, _____, the undersigned, am hereby submitting this Subscriber Agreement to the [*insert State/Commonwealth agency*] in application for a Personal Identity Number that shall, along with my username, password and additional personal security information, serve as the Electronic Signature Device and equivalent of my handwritten signature on all electronically submitted reports, documents, applications, files and forms to the [*insert State/Commonwealth agency*]. I hereby:

1. Agree to protect my electronic signature device and security question/answer pairs from compromise and from use by any other party, including anyone who may be acting as my agent;
2. Promptly report (within 24 hours after discovery) to the [*insert State/Commonwealth agency*] any evidence of the loss, theft, or other compromise of this electronic signature device and/or security question/answer pairs;
3. Review and, if necessary, repudiate, any electronic reports, documents, applications, files and forms that may have been submitted to the [*insert State/Commonwealth agency*] after this loss, theft or compromise;
4. Promptly review (within 24 hours after discovery), the acknowledgements (email and onscreen) and



copies of submitted documents using this electronic signature device, and;

- 5. Promptly report (within 24 hours after discovery) evidence of discrepancy between any electronically submitted information signed using this electronic signature device and what was received by the [insert State/Commonwealth agency]'s electronic receiving system.

I understand that I shall be held as legally bound, obligated, and responsible by the electronic signature created using this electronic signature device as by my handwritten signature.

Applicant Signature: _____ Date: _____

NOTE: Notarization is optional

Notarization of Electronic Signature Device and Subscriber Agreement

In the State of: _____

and the County of: _____

On _____ before me, _____, (date of signing) (Notary's name)

personally appeared _____, personally known to me (or proved to me on the basis of satisfactory evidence) to be the person whose name is subscribed within this instrument and acknowledged to me that he/she executed the same in his/her authorized capacity and that by their affixed signature on this instrument do affirm their lawful execution thereof.

Witness therefore my hand and official seal (Notary Seal)

(Signature of Notary)