SecureDoc
MODEL STANDARD OPERATING PROCEDURE

I. Purpose:

This standard operating procedure establishes the purpose and parameters under which the agency will use the SecureDoc application for reviewing documentation and procedures associated with businesses regulated by the agency.

II. Use of SecureDoc:

The agency may use SecureDoc to review a regulated firm's procedures, food safety plans, or other documentation in the following circumstances:

A. For purposes of gaining a better understanding of the facility's food products, processes, and food safety system, to better prepare for and prioritize an upcoming onsite inspection;
B. For purposes of reducing the amount of time spent in the plant conducting procedural and documentation reviews as part of an onsite inspection; or
C. For purposes of evaluating the firm's food safety systems and controls, to help determine if a full on-site inspection is currently warranted.

The agency will not utilize SecureDoc to remotely review Food Defense Plans or records associated with the monitoring, verification, or corrective actions that document implementation of the firm's food safety plan. These plans and records should not be requested for remote document reviews due to their sensitivity or the potential volume of individualized records that would have to be assembled and uploaded.

III. Communication with the Firm:

Initiating the Request: The inspector assigned to conduct a remote regulatory document review, whether or not the review is part of an onsite inspection assignment, shall make contact with the firm's point of contact (POC) to initiate the process. The firm's POC may be identified either through the firm's FDA registration, the state's licensing database, or by contacting the firm directly and communicating with the firm's management team to determine who the POC will be for the assignment. Contact with the firm and initiation of the request may be made in the one of the following ways:

A. Through an in-person visit to the business which includes the presentation of credentials, and presentation of the request on agency letterhead.

B. Through correspondence on agency letterhead that is mailed to the business, and followed by a phone or virtual meeting discussion with key firm officials to review the request and identify the firm's POC for the review.
C. Through an email presentation of the request from a state verified email address, with an authentication process built-in, such as a telephone verification with the main office switchboard or program management. This contact should also be followed by a phone or virtual meeting discussion with key firm officials to review the request and identify the firm's POC for the review.

Pre-Review Call or Meeting: The inspector and firm's POC should have a pre-call, webinar, or meeting to discuss the purpose for the remote document review and to discuss the scope of the documents being requested. The POC should be requested to provide a brief overview of the products produced and handled at the firm, an overview of the process flow of the products of interest, and the format of their food safety plan and written procedures, to assist the inspector in narrowing the scope of the documents requested for review. The inspector should introduce the SecureDoc application and discuss the security framework set up around the documents that the firm will upload. Only documents that are relevant to the assignment should be requested.

Ongoing Communications & Closeout Discussions: Communication between the inspector and the firm's POC should occur routinely throughout the review process to assure documents are considered and evaluated within the appropriate context. The inspector and POC can agree to use the secure comments function within SecureDoc to clarify information and ask questions, or can schedule periodic follow-up conference calls or webinars to obtain clarification and discuss potential concerns.

The inspector and facility POC should also have a debrief or closeout meeting at the conclusion of the remote document review or during the onsite inspection if the review is conducted as part of an onsite inspection assignment.

IV. Written Correspondence Requesting Remote Document Review:

Remote document review through an online application is new to most companies and has not been a method traditionally used by regulators as a part of their inspectional processes. While state law may not specifically require a written request to review documents under the state's inspection authority, as a courtesy and to ensure uniform application of the process, the agency will issue written correspondence to initiate the request for remote document review. The correspondence or written request should include the following key elements:

A. Brief introduction to the purpose of the correspondence;
B. Introduction to the SecureDoc software as a secure means to remotely review procedures and documentation;
C. Identification of the types of documents that will be requested, the purpose for the request, and how the review will be used;

D. Identification of the inspector that will be contacting the business to discuss the request, answer the business's questions, and be reviewing the materials provided by the firm. The inspector's contact information should also be provided;
E. Timeframe for the review;
F. Whether the review of documents will or will not be associated with an on-site inspection;
G. How questions regarding the documents will be discussed with the business;
H. How deficiencies identified during the remote document review will be communicated with the business;
I. Identification of one or more methods to verify the identity of the inspector that will be reviewing the documents. This may be accomplished by providing the main program phone number that can be verified on the internet or through a local phone directory and called to verify that the inspector does in-fact work for the agency, or by meeting with the company via webinar and having the inspector present their credentials while the inspector's video camera is on;
J. Identification of the method that hard copies of specific documents or sections of documents will be requested if necessary once the remote document review has been completed.

V. Responsibility of the Inspector:

Inspectors shall adhere to the following practices when conducting remote document reviews:

A. All documents uploaded to SecureDoc shall be reviewed in a secure manner by the authorized inspector, and protected from unauthorized access.
B. The authorized inspector shall not share the link or password to the documents uploaded to SecureDoc with anyone that has not been assigned by agency management to review the documents.
C. Only agency personnel that are authorized and have been identified in advance to the firm whose documents have been uploaded to SecureDoc, shall review or have access to the uploaded documents.
D. Inspectors shall not take screen shots, pictures, or in any way capture images of the documents they are reviewing through SecureDoc, unless the firm has specifically provided unrestricted access to the document and has opted to share official copies of the documents with the regulatory program through the SecureDoc portal.
E. When an inspection of the facility will be conducted as part of the remote document review, the inspector conducting the remote document review should also complete the on-site component of the inspection.
F. The initiation or conclusion of an on-site inspection that is conducted in connection with a remote document review should occur within 30 days of the completion of the remote document review.
G. If major food safety issues are identified during a remote document review activity, the inspector shall notify their supervisor, discontinue the remote document review activity, and initiate an on-site inspection.

VI. Documentation:

Remote document review activities that are associated with an on-site inspection shall be documented in the inspection report that is associated with the on-site inspection. Deficiencies or concerns identified during the remote document review shall be discussed with firm management, giving them an opportunity to explain any potential misinterpretation of the information reviewed. Significant findings or violations will be documented in accordance with agency procedures at the conclusion of the inspection via a notice of violation (FDA 483 equivalent).

Documenting the remote document review in a stand-alone report will only be necessary when the remote document review is conducted as a stand-alone activity and is not associated with an on-site inspection. Significant findings or violations identified during the remote document review shall be provided to the firm through regulatory correspondence or in person via a notice of violation. Minor deficiencies may be presented to the firm during a close-out teleconference or webinar and used as an opportunity to educate the firm on the applicable regulation, while providing them time to make the corrections before the next scheduled on-site inspection, when the corrective actions can be verified.

VII. Providing Standardized Instructions for Uploading Documents:

All firms that are requested to upload documents into SecureDoc for remote document reviews must be provided with clear written instructions on how to access SecureDoc, upload documents, and set controls for those documents. The controls on the documents are established by the business that will be uploading the documents, but the agency must provide guidance on how to set those controls to ensure the remote document review can be completed effectively. Instructions may include language similar to:

The use of SecureDoc allows industry users to securely share documents with regulatory officials. The process is initiated by accessing SecureDoc at: https://www.securedoc.app/my/login/exit.cfm. First time users should select "create account" on the log-in screen and register for use of the site by entering their requested contact information. A password will be generated and sent to the user upon registration approval. Returning users can log-in through the sign-in screen by entering their user name and password. Once logged in, follow these procedures:

A. Select the "**Dashboard**" tab from the left column directory and click on the "start" button under "Upload File" section on that page. This will open the "Send Files" screen to establish the controls for the file(s) that will be uploaded.
B. Users should establish the following security controls:
   1. Set the date in the "**Date File Expires.**" *(The inspector should provide the date for this field based on the standard timeline for document review established by the agency or the specific date based on the volume of documents to review.)*

2. "**Retention**" category - select the checkbox "Remove File After Expiration" so that the file will be deleted in accordance with the settings for the file (such as the file expiration date).
3. "**Require Password**" category - select the checkbox to enable a password for the file. Passwords are generated automatically and displayed for the user immediately after the file is sent. (*This is optional as an added layer of security*)
4. "**Restrict View**" category – The system automatically restricts uploaded files to "view" only so that reviewers cannot print, copy, or download any of the uploaded files. If the user wishes to allow the documents to be downloaded or printed, they must uncheck the box in this section.
5. Select "Enable" in the "**Limit Views**" category and enter the number of views that will be allowed If users wish to place a limit on the number of views that an authorized viewer can access the document before the date the file expires. *(Use of this field will limit the number of times that the inspector can access the file before they are locked out. Consideration should be given for how many interruptions might occur during the review process when recommending a number of views to the firm. The agency may opt to ask the firm not to limit the number of views and just rely on the expiration date for the review limits.)*
6. Enter the e-mail address(es) for the agency personnel that will be authorized to review the documents in the **"Email Addresses"** field. *(The emails should be provided by the assigned inspector)*
7. Enter any e-mail message in the **"Email Message"** field that you want sent to the authorized viewers notifying them that the files have been uploaded.
8. Click on the "**Select Files**" button and browse through your folders and select the files to be uploaded to the cloud and associated with the security protocols established.
9. Select "**Preview Email**" button if you wish to review the email language prior to sending.
10. Select the "**Send Email**" button to send the email to the email addresses that were entered. A pop-up screen will appear showing the user the security controls they have placed on the documents that were uploaded. Users can either select the "change options" button to return to the "Send Files" screen and update the security settings before sending the email / file link or select the "Send Now" button to send the email with file link to their selected recipients. The following screen that appears will confirm that that the document links were sent and will provide the randomly generated password that was established to access the file, if that option was selected.

C. Transmit a separate e-mail or text (outside of the SecureDoc application) to the individual(s) that you authorized to access the file with the auto-generated password that was established for the file(s).

Users can monitor the files they have uploaded under the "My Files" tab. Information related to the file(s), including the date uploaded, the expiration date of the file, and when the file was accessed by the authorized viewer is available. Once the parameters have been met with regard to file retention, the file will be deleted from the secure server and the drive wiped.