Safeguarding Customer Information & Company Data

Reference Guide

CITADEL
SERVICING CORPORATION

CSC – Standards for Safeguarding Customer Information

CSC requires all borrower electronically transmitted information and communication to comply with CSC's Electronic Communication Consent Agreement.

CSC requires encryption or password protection of sensitive customer information when it is transmitted electronically via public networks and is not under the purview of CSC's Electronic Communication Consent Agreement.

CSC – Standards for Safeguarding Customer Information

All calls or other requests for customer information must be directed to designated individuals who have been trained in how the company safeguards personal data.

Any documentation including, but not limited to, the following information is to be placed in “shred” bins: Social Security Numbers, Names and Addresses, Property or Mailing Addresses, Loan Numbers, Bank Account Numbers, Credit Card Numbers, Employer’s names, addresses or phone numbers, Credit status or history, Employment status or history, Corporate Proprietary Information.

Third Parties and Agents

CSC's role in any loan transaction is to qualify and provide financing for the applicant's for credit. Sensitive applicant information is to be provided only to the applicant, using a secure method of communication. The applicant is free to share any information with other parties at their discretion.

CSC will provide other service providers with information related to the transaction only when deemed appropriate and always using a secure method of communication. Title and Escrow Companies, AMCs, Hazard Insurance Providers, etc. may request information as parties in the transaction. CSC will provide only provide information necessary for them to carry out their specified responsibilities toward loan closing.

Third Parties and Agents

In purchase transactions, the seller and seller's agent are not to be provided with sensitive borrower information. The borrower may provide information at their discretion. General information related to the timing of consummation, or terms specific to the seller are acceptable to share as long as CSC's Standards for Safeguarding Consumer Information are followed.

Official Contact Information

CSC employees should only provide information to official email and office addresses.

- E.g. SharonFidelity@gmail.com would not be an acceptable email address to send sensitive borrower information. An alternate email address with an official domain name should be requested. (Sharon@Fidelity.com)

A mailing address which is unable to be verified via public information should be verified by contacting the company directly.

- E.g. If a representative requests that information be mailed to an address other than a listed place of business for the title company, additional verification via phone or email should be conducted.

System Integration Requirements

CSC has integrated certain functions into existing technology such as Ordering Credit, Opening Title, Obtaining Flood Insurance etc.

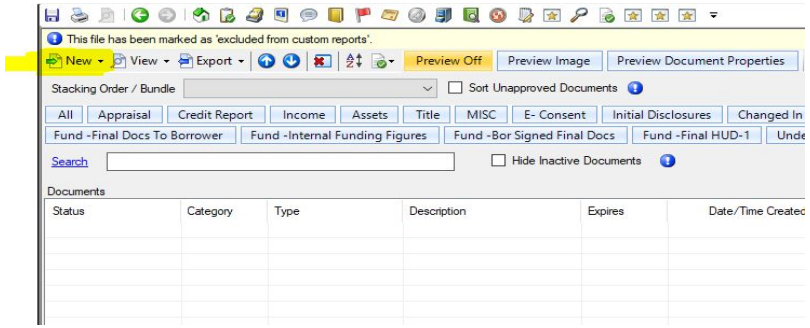
These functions should be utilized at all times (unless directed by Senior Management).

If a request is made to complete any process which is normally integrated or password protected, it should be escalated to a manager before proceeding.

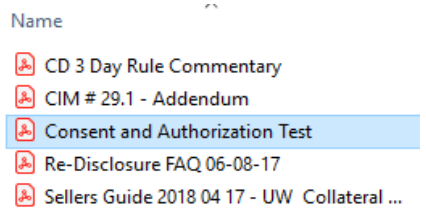
Password Protecting Documents

Using the “Stored Documents” screen:

1. Click the “New” button in the upper left corner

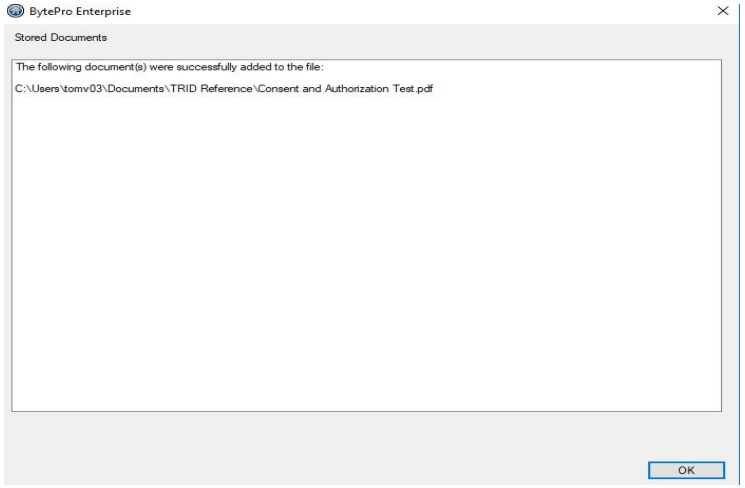


2. Select “Import new documents from disk” from the dropdown menu.
3. Select the desired document from the folder in which it is saved.

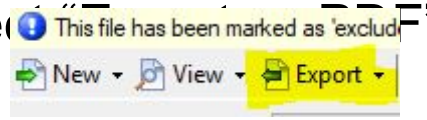


Password Protecting Documents Cont.

- Click the “OK” button when the acknowledgement displays the successfully added message.



- Highlight the desired document from the list of Store Docs
- Click the “Export” button and sele “ DF” from the dropdown list.



Password Protecting Documents Cont.

- Select “Protect Documents with a Password” and enter “Citadel[last 4 of borrower’s SSN]”

E.G. Citadel1234

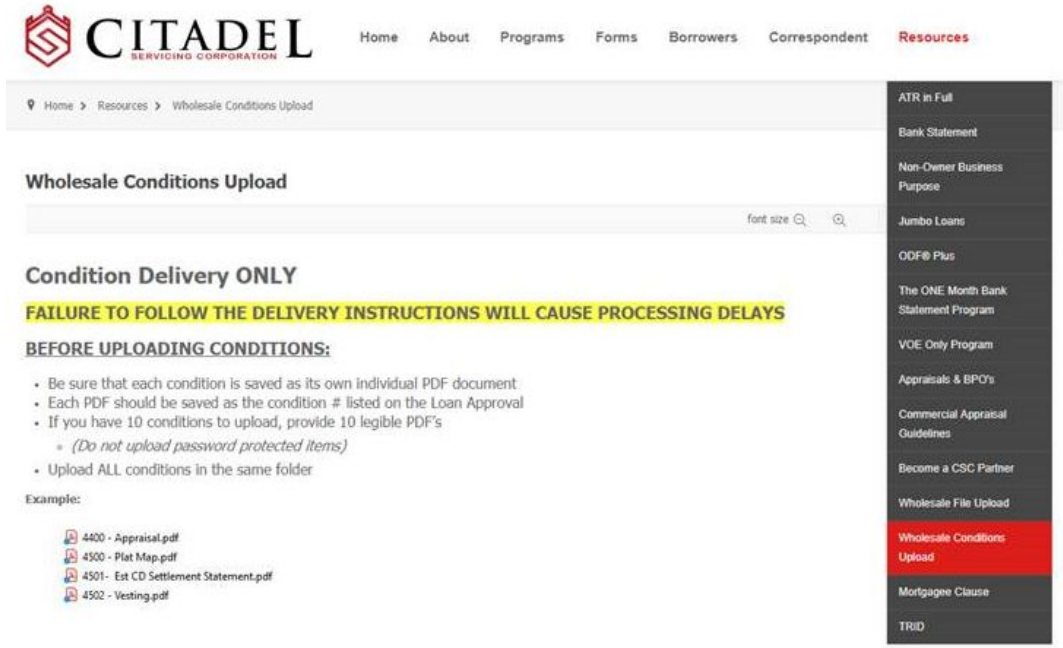
- Click the OK button and the password protected PDF document will be saved to the computer. Passwords to documents should be sent in separate emails for security purposes.

Password Protecting Documents Cont.

TM's:

For outbound items containing confidential information they should be using the password encryption in ByetPro. Outbound items are not shared through Box.

For incoming conditions and other borrower information, they should be encouraging the Brokers and their Processors to upload via the CSC website, which in turn uploads it to Box. Screen shot is below.



Safeguarding Company Data

Safe Guarding your Work Station

In addition to the policies and procedures that help fight against financially fraudulent activity, there are also practical ways to prevent them.

- Whenever you leave your work station or laptop unattended, **always lock your computer when you walk away from your desk!**

- Periods of Computer Inactivity: set up your screen saver to become active after 2 minutes of work station inactivity.

Safe Guarding your Work Station

- Do not bring in USB sticks, plug your phone in to your PC, download anything unrelated to work, or give anyone access to your PC that isn't affiliated with CSC.

- Any documents should not be left out in the open on your desk.

- Always keep you Key FOB secure. Notify HR if it is lost or has been stolen so it can be disabled.

Technical Safeguards

- Do not open Links via email if it is not intended for you, **OR** if you do not know the recipient. Phishing Emails intended to misguide or trick you.

- **Phishing** is a fraudulent attempt, usually made through **email**, to steal your personal information. **Phishing emails** usually appear to come from a well-known organization and ask for your personal information — such as credit card number, social security number, account number or password.

Technical Safeguards

- And DO Not enter in personal information from a Spoofed Website upon clicking on links. Asking you to sign into work related accounts. (Office365 as an example when your already logged in!)

- A **phishing website** (sometimes called a "spoofed" **site**) tries to steal your account password or other confidential information by tricking you into believing you're on a legitimate **website**. You could even land on a **phishing site** by mistyping a URL (web address).

Administrative Security

- Times out after 3 attempts and You will not be able to log back into your workstation for 15 min.
- Multi-Factor Authentication (MFA) for Office365 email. For your desktop client and for your Devices as well. Pushes SMS or VM to verify your identity with a numeric code.
- End Point Security Cylance will notify I.T. if you have downloaded any malicious software. Or that is considers malicious. Could be intentional download or unintentional.
- Please contact IT in response if you have or think you might have accessed or received a virus.

Any Questions?