

**Information Security Program
Information Security Access Assessment – Branch Office Assessment**

Branch # _____

Date _____

A. EMPLOYEES:

1. List all new employees (Lending & Operations staff) and their positions that have been in your office since the last Information Security Access Assessment. Indicate if they have signed the Employee Acknowledgement to the Employee Guide to the Information Security Program:

| <u>NAME</u> | <u>POSITION</u> | <u>Acknowledgement Signed?</u> |
|-------------|-----------------|--------------------------------|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

2. Have the above employees been granted ITI access at a level appropriate for their position?

Yes

No

Please explain any "No" answers:

3. Has the ITI access level been changed for any employees in the last 6 months:

Yes

No

Please explain any "Yes" answers:

B. CUSTOMER INFORMATION

1. Is customer information kept in a secure area at night such as the vault, a locked cabinet, drawer, or locked office? (*Customer information includes reports, loan files, signature cards, account documents, and any other item that contains confidential customer information.*)

Yes

No

Please explain any “No” answers:

2. During the day, is customer information kept where an unauthorized person cannot easily view or take such information?

Yes

No

Please explain any “No” answers:

3. In the “Platform” area, are password protected screensavers used to prevent screen information from being accessed if an employee is away from his or her desk?

Yes

No

Please explain any “No” answers:

4. Is any confidential information left in the trash at night instead of being placed in the shred bin?

Yes

No

Please explain any “Yes” answers:

5. Do all employees place shred items into the shred bin at the end of the day?

Yes

No

Please explain any “No” answers:

C. PASSWORDS AND LAPTOPS

1. Are passwords kept in a secure location? (*Passwords should NOT be placed on or near the computer workstation either on the monitor, underneath the keyboard, next to or near the computer.*)

Yes

No

Please explain any “No” answers:

2. Are employees instructed NOT to use a password that is easily guessed? (*Examples of easily guessed passwords include employee names, the name and/or number of the branch, or an easy series of letters or numbers such as 1111, 12345, abcde.*)

Yes

No

Please explain any “No” answers:

3. Are all laptops kept in a secure location at night? (*Laptops should NOT be left in an unlocked location such as a desktop or unlocked drawer unless it is inside of a locked office.*)

Yes

No

Please explain any “No” answers:

D. NEW ACCOUNTS, PRETEXT CALLING, & UPDATING CUSTOMER INFORMATION

1. Are New Accounts personnel advising customers on the use of the Automated Calling Center?

Yes

No

Please explain any “No” answers:

2. Do they advise customers to change their PIN the first time they use the system?

3. Yes

No

Please explain any “No” answers:

4. Are they giving the Privacy Disclosure brochure to all new CONSUMER account customers?

Yes

No

Please explain any “No” answers:

5. Are New Accounts personnel obtaining acceptable Primary and Secondary identification for all new customers? *(See Section 105.1 of the Operations Policy Manual)*

Yes

No

Please explain any “No” answers:

6. Do all personnel have an understanding of what Pretext Calling is? *(See the Employee Guide to the Information Security Program. This should be covered periodically during staff meetings.)*

Yes

No

Please explain any “No” answers:

7. Do employees know how to properly identify customers before giving out information? *(This should be covered periodically during staff meetings.)*

Yes

No

Please explain any “No” answers:

8. Do employees know NOT to give out customer information just because the caller states they are an attorney or law enforcement? *(All such calls should be referred to a supervisory level person and, if necessary, to Operations Support. Attempts at Pretext Calling may require the filing of a Suspicious Activity Report.)*

Yes

No

Please explain any “No” answers:

9. When an address change is requested, is the customer’s identify verified before the address change is made?

Yes

No

Please explain any “No” answers:

10. When customer information is entered or changed on ITI, is there an independent call-back to verify the information was entered accurately?

Yes

No

Please explain any “No” answers:

I certify that I have reviewed the Information Security practices in this branch office and have reported the findings in this Information Security Access Assessment – Branch Office Assessment.

Customer Service Manager - Signature

Date

Business Center Manager – Signature

Date