Table of Contents

Table of Contents i
2-90 Information/Cyber Security Plan and ID Theft Plan Overview 1
Laws Governing Compliance 1
What's Required and How We Comply 2
2-90-01 IT Plan Components 3
Areas of Risk 3
2-90-10 Scope of Information Technology (IT)/Cyber Security and Identity Theft Plan 4
Identity Theft Defined 4
Protected Non-Public Personal Information (NPI) Defined - Classification 4
Examples of Public and Non-Public Information 4
Document Retention Scope 6
Part 1 - Written Information Security Plan (WISP) to Protect Consumer Information 7
Part 2 - Red Flags Plan to Identify Fraud Quickly 7
2-90-11 IT Plan Personnel and Duties 8
Listing of Information Security Personnel 8
2-90-13 Information Security/ID Theft Officer Duties and Responsibilities 8
Updating the Program 9
Third Party Audit Firm 9
2-90-20 Employee Responsibility 10
System Monitoring 10
2-90-21 - Office Security 11
2-90-22 Physical Office Security – Employees and Visitors 13
Keys, Key Cards or Other Office Access 13
Security Systems 13
2-90-23 Controlled Access by Job Duty 14
2-90-24 Password Security 15
2-90-25 IT Device Security - Desktops, Laptops and Mobile Devices 16
Desktop Workstation Computer Security 16
Laptops and Mobile Devices 17
FORM 2-90-25 IT Security Inventory 18
"Patch" Management Procedures 19
Managing Patches 19
2-90-30 Electronic Communication 21
Truncating Social Security Numbers on Requests 22
Confidential Information 24
E-Mail Signature Disclaimer 25
Secure Fax Transmission 26
2-90-31 Avoiding Email Scams 27
2-90-40 Secure Telephone Communications 28
2-90-50 Document Retention and Destruction 29
Document Retention 29
Document Destruction 29
General Records Retention Schedule 30
Onsite Paper Records Storage Policy 32
2-90-60 Training Programs 33
Manager - Initial Training 33
All Staff - Initial Training 33
All Staff - Annual Training 33
Required Training Topics 33
2-90-7 Malicious Code Prevention 35
2-91 Information Security Audit 36
2-91-1 Vendor Approval and Review 36
2-91-2 Information Security Questionnaire 38
Resolution of Audit Findings 42

2-92 Data Breach/Incident Response Policy and Implementation Guide 43
Definition of Breach/Incident 43
2-92-1 Reporting Breaches/Incidents 44
Reporting a Data Breach 44
Assessing NON-PUBLIC PERSONAL INFORMATION (NPI) Loss Risk Associated with a Data Breach 45
Completing the Analysis and Report 46
Assigning Risk Score 48
Non-Notification, or Notification and Remedy to Impacted Individuals 48
Timing of Notification 48
Responsibility for Notification 48
Content of Notification 49
Method of Communication 49
2-92-2 Process for Remediation of a Breach 50
2-93 Red Flag Identity Theft Plan 51
Covered Transactions - Defined 51
Are we a High-Risk Entity? 51
Fraud and Red Flag ID Theft 51
2-93-10 Identity Theft “Red Flags” 52
Victim or Perpetrator? 52
Steps we take to Detect Red Flags 52
2-93-20 Red Flag Discovery and Process 53
Red Flag ID Theft Issues Report 54
Working with Customers who have Identity Theft Problems 55
2-93-30 Procedure upon Red Flag Alert 56
Preparing the Identity Theft Affidavit-Police Report 57
Completing A Suspicious Activity Report (SAR) 61
2-93-3 Program Training Requirements - Avoiding Redundant Training Burden 62
Mortgage Fraud and Identity Theft 62
2-93-4 Red Flag Risk Assessment 63
Risk Assessment by Category 63
2-94 Secure Remote Access Policies and Procedures 64
Secure Remote Access 64
End-Point Security 64
Remote Access Hardware Usage 65
Company Provided Hardware 66
Payment and Reimbursement for Remote Access Expenses 67
Reimbursement for travel to Physical Location 67
2-94-1 Document and Private Information Security 68
Email Usage 68
Printer and Scanner 68
2-94-2 Remote Supervision 69
One-on-One Meetings 69
Company Meetings 69
2-94-21 Maintaining Proper Time Keeping Records 70
Work Schedule 70
Time Monitoring 70
Device Activity Monitored 70
2-94-3 Virtual or In-Person Client Meetings 71
2-94-4 Onboarding and Annual Review of Remote Staff 72
Completion of Onboarding/Review Checklist 72
Testing of Remote Work Environment 74
2-95 IT Plan - Training and General Implementation 75
The ID Theft Epidemic 75
Identity Theft vs. Identity Fraud 75
Common Identity Theft Schemes 76

Identifying Potential Fraud Quickly 76
"Vishing" 76
Social Engineering Scams – Internal and External Prevention 77
FTC Red Flag Matrix 79
Working with Borrowers - Counseling the Public 80
Advising Consumers on Strategies to Deter Identity Theft 80
2-96 Vendor IT Security Risk Assessment 81
Risk from Vendors 81
Information Transfer to Investors and Private Mortgage Insurance Companies 84
Information Transfers to Credit Bureaus 85
Information transfers to Appraisers 86
Information Transfer to Attorneys and Title Companies 87
Closing Agent Risk Assessment 87
Website and Loan Origination (IT) Software Vendors 88
2-97 Disaster Recovery and Business Continuity 89
Purpose of the Business Continuity Plan 89
Maintenance 90
Testing 90
Disaster Planning and Preparation 91
Emergency Planning Checklist 91
Testing the Plan 93
2-97-1 Organization of Disaster Response and Recovery 95
Disaster Response 95
Disaster Level Determination 95
Disaster Notification 95
2-97-2 Recovery Procedures 96
Activation of Continuity Plan 97
Recovery – Return to Business as Usual 98
2-97-3 Fire Drills 99
2-97-4 Data Backup and Recovery Methods 100
Daily Backup Schedule 100
2-97-5 Pandemic Preparation and Policies 101
Pandemic Preparation 101
Employees Encouraged to Work Remotely 101
Identification of Key Employees 102
2-97-6 Notification to Business Partners and Public - Pandemic 103
Sample Open Letter - Statement of Response 103
2-97-7 Pandemic Risk Assessment 104

2-90 Information/Cyber Security Plan and ID Theft Plan Overview

Our objective in this Written Information/Cyber Security (WISP) and Red Flag Identity Theft Plan (the plan, or Information Security Plan of Red Flag ID Theft Plan) is to identify areas of risk within our operation, understand our obligations under the law, and to have formal procedures for resolving issues that arise with respect to sensitive consumer information.

A Red Flag ID Theft program identifies a customer who may be a victim through theft or data breach. An information/cyber security plan (WISP) works to prevent theft and data breaches in the first place.

Laws Governing Compliance

Law	Description
FACTA	Fair and Accurate Credit Transactions Act requires all financial service firms, including mortgage companies and mortgage brokers, to have a “Red Flag” program to identify whether consumers may already be victims of identity theft.
GLB	Gramm-Leach-Bliley Act GLB rules overlap with FACTA rules for safeguarding sensitive customer information, records retention and document destruction.
Sarbanes - Oxley	Document Retention Rules Sarbanes - Oxley rules define what we must keep and for how long.
FCRA	Fair Credit Reporting Act Defines customer rights and our obligations for information reported in or to credit reporting agencies.

The regulations provide companies with some flexibility in developing internal programs according to their relative organizational size and complexity. We seek to avoid risks associated with ID Theft and data breach.

2-90-10 Scope of Information Technology (IT)/Cyber Security and Identity Theft Plan

Because we have access to sensitive consumer data, we must take aggressive proactive measures to secure customer information and combat ID theft when we see it.

Identity Theft Defined

Identity theft - Access of Non-Public Personal Information (NPI) without permission.
Identity fraud - When identity theft results in a crime for financial gain.

Protected Non-Public Personal Information (NPI) Defined - Classification

NPI is:

- any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, ***or other information on an application***);
- any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
- ***any information you get about an individual in connection with providing a financial product or service*** (for example, information from court records or from a consumer report).

The specific amount and extent of Nonpublic Personal Information (NPI) we request, retain and share varies greatly depending on the scope of the transaction.

Examples of Public and Non-Public Information

Public Information – From Lists or other public information	**Non-Public Private Information**
Employee Information Telephone numbers Mortgage holder on particular property Name Employment/Income terms for public employees (e.g., government institution.) Employee ID number Salary Gross pension Value and nature of fringe benefits Expense reimbursements Job titles Job description Education and training Previous work experience First and last employment Existence and status of complaints Terms of buy-out agreements Final disposition of disciplinary action	Any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application); Transaction information Social security number Personal Financial information Account numbers Trade secrets or intellectual property such as research activities Birth date Home phone number Home address Health information Location of assets Passwords Gender Ethnicity Citizenship

2-90-25 IT Device Security - Desktops, Laptops and Mobile Devices

Desktop Workstation Computer Security

We take appropriate measures to ensure the confidentiality, integrity and availability of sensitive information, including restricting access to sensitive information to authorized workstation users. Personnel must act to protect sensitive customer information and limit the possibility of unauthorized access.

Workstations include laptops, desktops, PDAs such as tablets, pads and readers, or any other computer-based equipment containing or accessing customer and company information directly or via network. This includes physical office workstations and authorized home workstations.

Personnel must

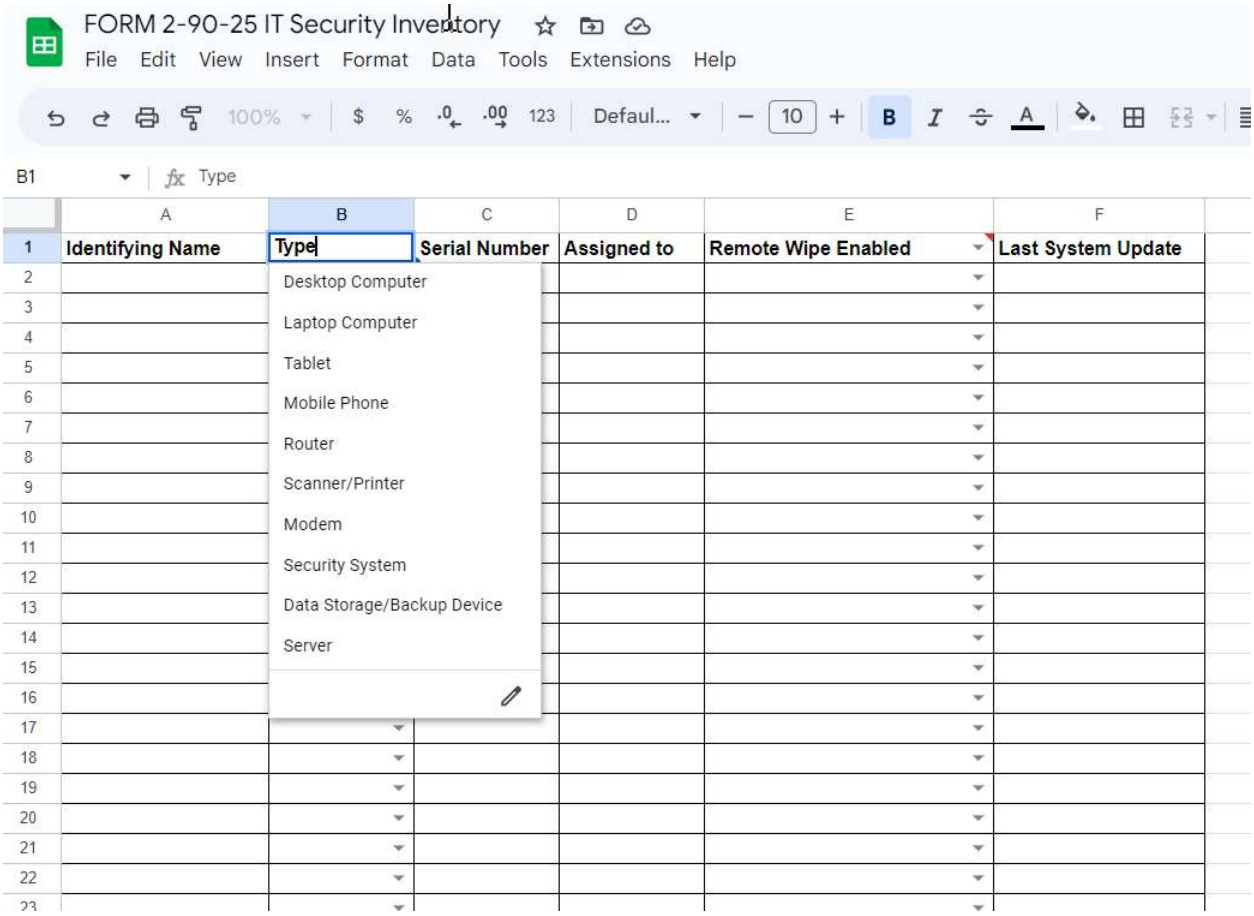
- Restrict physical access to workstations to only authorized personnel - never let anyone else use your desktop or digital equipment.
- Secure your workstation (screen lock or logout) prior to leaving workspace by
- Enabling a password-protected screen saver with a short timeout period
- Complying with all applicable password policies and procedures.
- Ensure you use your workstation for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Store all sensitive information on network servers
- Keep food and drink away from workstations in order to avoid accidental spills.
- Secure laptops not in use with cable locks or lock laptops up in drawers or cabinets.
- Ensure your workstation has data encryption
- Install and update company Anti-Virus software
- Position monitors away from public view or install a privacy screen filter or other physical barriers to public viewing
- After hours
- If applicable, leave your workstations powered on but logged off in order to facilitate after-hours updates.
- When leaving exit running applications and close open documents
- Ensure that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the Wireless Access policy

Definitions

Term	Definition
Cleartext	Unencrypted data
Full disk encryption	Technique that encrypts an entire hard drive, including operating system and data
Key	Phrase used to encrypt or decrypt data
PDA	Personal Data Assistant.
Remote wipe	Software that remotely deletes data stored on a mobile device.

FORM 2-90-25 IT Security Inventory

We always maintain a list of all technology items in use. Hardware has a useful end of life when it no longer is supported by the software we run.



2-

FORM 2-91-1 IT Vendor Review Checklist

For companies who do not have any proprietary information technology, but utilize software and services provided by vendors exclusively, we rely on:

1.) the qualified audits of the technology provided by these vendors
2.) the fact that the institution is regulated by a similar authority and thus has security measures
3.) confirmation of ISO 27001 or similar
4.) Vendor is not chosen by us (required use) thus certification is up to third party

Vendor Category	Vendor Name	1. Vendor Audit certification	2. Supervised	3. ISO or similar	4. 3rd Party Vetting
E-Mail					
Loan Origination System					
E-Disclosure					
Data Backup					
Web 1003 Application					
Pricing and Eligibility					
Document Management					
EFax					
Voice-Mail/Telephony					
Network/Internet Service					
Office Support/Cleaner/Landlord					
Courier					

Audited by:

_____
Name/Title/Date

FORM 2-91-1 IT Vendor Review Checklist
2/7/23

In addition, we assume that other licensed entities with which we do business have had their plans reviewed and found acceptable. Consequently, we do not audit our mortgage lender business partners.

2-91-2 Information Security Questionnaire

5/29/2019 2-91 IT Security Assessment - Policies and Procedures

2-91 IT Security Assessment - Policies and Procedures

We are concerned with the security of consumer information. Not maintaining confidentiality, integrity, and availability of information can result in direct harm to consumers and operational and reputational risk for businesses.

* Required

1. **Do you have WRITTEN Information Security, ID Theft and Safeguarding Policies and Procedures?**
   Mark only one oval.
   - Yes
   - No
   - Maybe

2. **If Yes, please upload a copy of your P&P's**
   Files submitted:

3. **Do you and your personnel have Customer Privacy, ID Theft and IT Security Training at LEAST annually?**
   Mark only one oval.
   - Yes
   - No
   - Maybe
   - Other: _____

4. **If yes, please upload a copy of all certificates and or Syllabi**
   Files submitted:

5. **Has data been classified based on the criticality/sensitivity of the information? Have you determined and documented what information needs to be protected/secured?**

   _____
   _____
   _____
   _____
   _____

https://docs.google.com/forms/d/11i5dDoGFvBEChBoNIbGla_1umQcuk0DzsTmXiEiQiaM/edit 1/4

access

Completing the Analysis and Report

FORM 2-92 Data Breach Analysis and Report

Customer Name _____
Date of Incident _____
Customer Residence State

1. How Breach Occurred	
	H - Online system hacked
	H - Data was targeted
	M - Device was targeted
	M - Device stolen
	L - Device lost
	Score
2. Data Elements Breached*	
	H - Social Security Number
	H - Financial account number
	H - PIN or security code for financial account
	M - Birthdate
	M - Government Issued Identification Number (drivers license, etc.)
	L - Name
	L - Address
	L - Telephone Number
	*A combination of identifying information and financial or security information should always be considered a high risk with high likelihood of harm occurring.
	Score
3. Ability to access data	
	H – paper records or electronic records in a spreadsheet that is not password protected
	M – electronic records that are password protected only
	L – electronic records that are password protected and encrypted
	Score
4. Ability to mitigate the risk of harm	
	H – no recovery of data
	M – partial recovery of data
	L – recovery of data prior to use
	Score
5. Evidence of data being used for identity theft or other harm	
	H – Data published on the web
	M – Data accessed but no direct evidence of use
	L – No tangible evidence of data use
	Score
	Final Score

Action			
	No Action	FTC Complaint	
	Notify ONLY	SAR	
	Notify AND Remediate	Fraud Report	

_____
Prepared by

_____
Date

5/29/2019

Red Flag ID Theft Issues Report

FTC Red Flag ID Theft Issues Report

Date _____

Customer Name _____
Address _____

Production Process Red Flags

☐ Credit Report fraud alert	☐ Notice of a credit freeze	☐ Credit Report address discrepancy.	☐ New accounts or inquiries.
☐ ID appears altered	☐ Photo ID doesn't match	☐ ID doesn't match other information.	☐ Other ID variances – signature, other
☐ Application altered	☐ NO ID, SSN match found	☐ SSN and Date of birth range mismatch	☐ Alias, fictitious address or another recognized scheme
☐ Suspicious address, cell phone, contact info	☐ Duplicate SSN, wrong SSN	☐ Addresses match other customers' accounts	☐ Unable to respond to additional info request
☐ Inconsistent personal information in-file	☐ Can't provide password challenge	☐ Returned mail with active transaction.	☐ Drastic change new loans, late payments, credit balances

Servicing/Loan Administration Red Flags (If Applicable)

☐ Drastic change in payment patterns, credit balances	☐ Inactive account with sudden activity	☐ Returned mail with active transaction.	☐ Customer states not receiving statements
☐ Unauthorized transactions on customer's account.	☐ Notification of fraudulent account	☐ Change of Address with new users	☐ Rapid Cash and Consumer goods advances
☐ Can't provide password challenge	☐ Unable to respond to additional info request	☐ Addresses match other customers' accounts	

Other ID Theft or Fraud Flag

Item: _____
Item: _____
Item:

Disposition

Field Recommendation		Risk Level	Action
Believe Customer is	☐ Victim ☐ Perpetrator	☐ High – Active Fraud – Identity Theft ☐ Medium – More than 3 Red Flags ☐ Low – 2 or fewer Red Flags	☐ Police Report/SARS and Remediation ☐ Recommend ID Theft Program ☐ Identify risks and Educate on ID Theft Process

Report Initiated By (Name) _____

Title _____

Date _____

Receive by Compliance _____ Date _____

By (Name) _____

Resolution Date _____

FORM 2-93-4 Red Flag Issue Report Form
Revised 5/29/2019

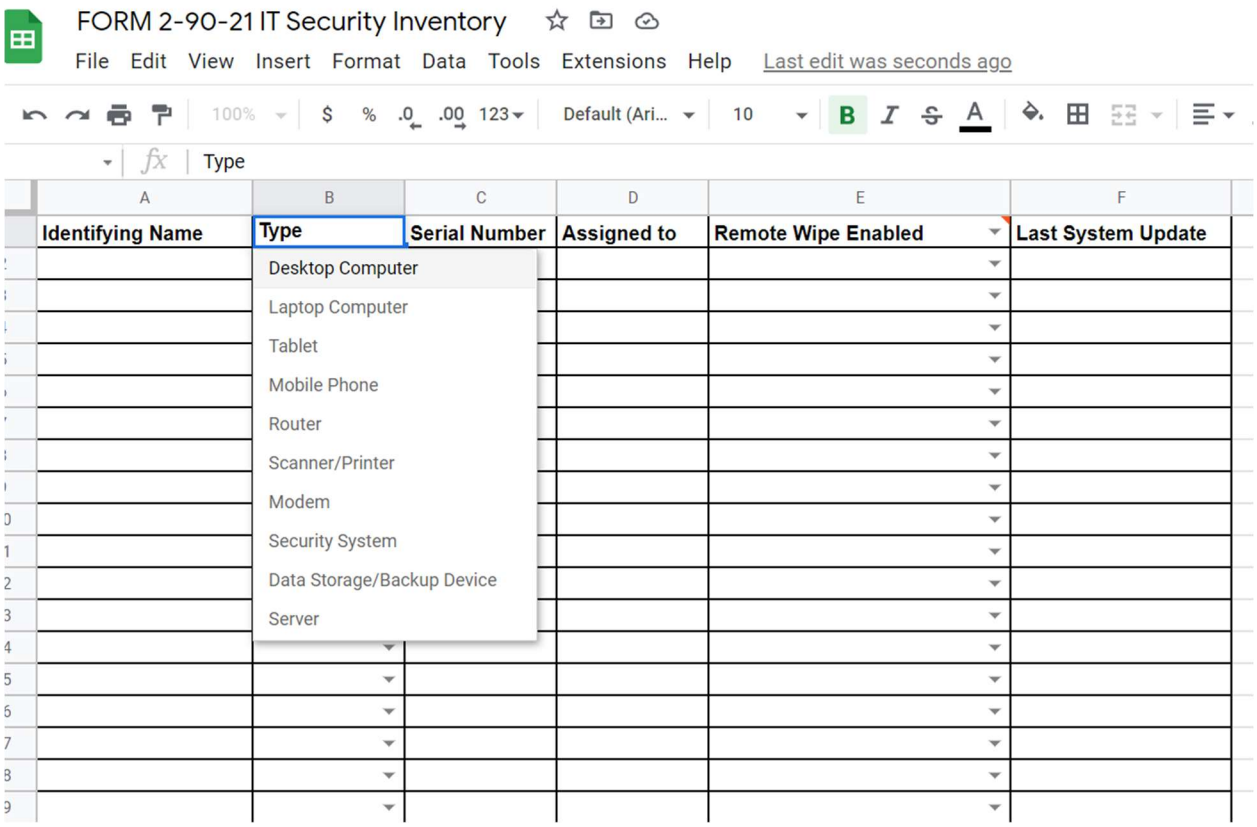
Remote Access Hardware Usage

Employees, whether fully remote or working remotely temporarily, must only access systems and perform work on Company approved and recorded devices. We discourage use of employees' own technology devices but will allow it provided

1.) the Company can remotely access the devices and control them.
2.) We have configured screen saver timeouts,
3.) Strong, dual factor password protection
4.) Encrypted hard drive

Employees who do not wish to allow this access to their devices may request a company provided item.

We require a complete inventory of all technology hardware utilized in remote work environments.



FORM 2-94-1 Remote Work Setup and Annual Review Checklist

Remote Worker Setup and Review

Remote Work Request and Authorization	
☐	Justification for Remote Work
☐	Company Authorization to Work Remotely
Hardware	
☐	Modem/Router
☐	Computer/Laptop
☐	IT Inventory
☐	
Secure Access	
☐	Location acceptable - locked door Credit Bureau
☐	VPN
☐	
Timekeeping and Administration	
☐	Remote Work Monitoring Agreement
☐	Remote Time Keeper (e.g. Quickbooks, Workpuls, etc.)
☐	Overtime/Remote Work Policy
☐	1 Hour - 10 minute break, 30 minutes for lunch - 8 hours per day
Loan Documentation	
☐	NO Paper Documents
☐	Bonded Shredding Service
☐	Secure File Document Upload Portal (e.g. sharefile, etc.)
☐	Wet-Signed Documentation ONLY to Main Office
☐	E-Sign Setup
Remote Resources	
☐	All physical work aids scanned and available on Intranet
☐	Intranet access to company specific documents
☐	Physical elements of office available online e.g. - Calendars, "Sticky Notes"
☐	
Oversight and Management	
☐	Daily, Weekly Virtual Meetings (e.g. Zoom, Webex)
☐	Company meetings
☐	Customer meeting secured location
☐	Annual Location Inspection

Review Completed by

Name _____

Date: _____

6/13/2023

1

Information Transfer to Investors and Private Mortgage Insurance Companies

Whenever possible files and should be transferred electronically via imaging software protocol. Often physical exhibits are transferred to the investor for review by underwriting. When this occurs we must be sure that the investor has information privacy and red flag detection program in place.

Responsible Party	Step	Description
Operations manager	Request confirmation investor has information security policy	No further investigation is required upon confirmation of red flag policy in place
Outside investor compliance officer	Provide verbal confirmation of red flag policy	
Processor, loan originator, underwriter	Deliver documentation via secure method	Choose secure delivery format-Federal express, UPS, or other Address specific individual Request signature confirmation

Risk Level

HIGH

FORM 2-97-1 Disaster Preparation Checklist/Pre-Drill Assessment

Disaster Preparation Checklist/Pre-Drill Assessment

Disaster Type

- ☐ Natural Disaster - Weather/Earthquake/Flood
- ☐ Fire
- ☐ Active Shooter/Workplace

Notification System

- ☐ Current Phone List - Last updated
- ☐ Local authorities numbers listed Police/Fire
- ☐ Group Text/Call Software
- ☐ Public Address

Special Needs System needed?

- ☐ Special needs persons accommodated Yes No

Physical Plant

- ☐ Evacuation routes posted
- ☐ Exits are clearly marked
- ☐ Illumination for assembly point & Exit Paths
- ☐ Fire pump work condition
- ☐ Fire Extinguishers wall mounted
- ☐ Exit doors operating properly
- ☐ Assembly point unobstructed
- ☐ Egress routes free of obstructions Yes No
- ☐ Egress routes properly lighted Yes No
- ☐ Emergency Supplies - First Aid/Water

Company Briefing

Sound of alarm steps

- ☐ Manager - Take Visitor Log
- ☐ Turn off workstation/save work
- ☐ Take personal effects
- ☐ FIRE CONTAINMENT
- ☐ Doors and windows closed
- ☐ Rooms checked prior to closing doors
- ☐ Restrooms Checked
- ☐ Doors left unlocked
- ☐ Electrical appliances were turned off
- ☐ Lights were turned off
- ☐ HVAC units were shut down
- ☐ Phones forwarded
- ☐ Email Autoresponder On
- ☐ How to Exit
- ☐ Where to meet

Post-Evacuation

- ☐ Customer Notification
- ☐ Website Announcement

3/11/2022