This document is provided to mortgage lenders as a courtesy, to assist them in instituting and maintaining data security policies that keep them in compliance with the Utah Division of Real Estate's administrative rule requirements. It is meant to be customized to fit each lender's specific operational procedures and needs. Effective policies give guidance and set operational boundaries for employees and are crucial to every data security plan.

To adapt this template and use it in your own company, use the following instructions:

- Each policy has three sections:
    - Purpose: Explains the purpose of that specific document
    - Scope: Defines who it applies to and when
    - Policy: The rules you set for your company
- Anything in red text is suggested to be customized and incorporated into your policy.
- Any light blue text is not meant to be included in the final version of your company's policy, but is instructional for the person setting up the policy.
- Suggestions within this template are not exhaustive. You should attempt to add additional points specific to your company's standard operating procedures.
- Policies are only beneficial when actively used. After customizing this template to fit your company, make sure your employees all have a copy of the policy and are aware of the new rules within it.

It is important to note that the completion of this policy alone does not guarantee your compliance with the Division's rules and regulations. It also does not necessarily satisfy any additional federal or state data security requirements including the GLBA Safeguards Rule and Utah's Cybersecurity Affirmative Defense Act, H.B. 80. To ensure complete compliance with all federal and state cybersecurity regulatory requirements, please consult with a professional data security firm.

[Your Company's] Data Security Policy Template

Policy Sections Include:

1. Customer Privacy Policy
2. Customer Information Security Policy
3. Password Management Policy
4. Cybersecurity Policy for Employees

1. Customer Privacy Policy

Purpose

The purpose of the customer Privacy Policy is to protect borrowers from having their data shared without their permission. This policy enforces the expectation that consumers have for their data privacy.

Scope

The Customer Privacy Policy applies to any employee, contractor, or individual with access to customer data.

Information that is protected by the Customer Privacy Policy includes:

- PII (info that directly identifies an individual, including address, name, ssn, etc…)
- Financial documents
- Signed forms
- Forms of ID
- Government or legal documents
- Client lists
- Anything else reasonably considered sensitive or private

Policy

1.1 Employees must not share any consumer information, documents, or data with any third parties without each consumer's clear consent.

1.2 Employees must not share client lists, email addresses, or other contact information with anyone without each consumers' clear consent, and only for a legitimate business purpose as it relates to closing a loan.

You should amend policy points 1.1 and 1.2 to accurately reflect who your company shares customer information with. You should also add additional points that define your customer data sharing practices.

2. Customer Information Security Policy

Purpose

The Customer Information Security Policy defines the standard operating procedures for handling customer data, as well as the measures taken by the business to protect that data.

Scope

The Customer Information Security Policy applies to any customer data or documents. All employees, contractors, and other individuals with ties to the business are required to be informed of and operate within the boundaries set by this policy.

Policy

In this section, you will first define how your employees request, accept, store, and transfer customer data. This is different for every mortgage shop. The most important part is making sure that whatever you include in this policy matches how your business actually operates. Next, you should outline specific prohibited ways of handling customer information.

The following points in red are examples, and should be edited and expounded on in order to mirror your company's operations.

2.1 Employees must request customer documents and data be sent through (insert secure portal/service).

2.2 Customer data must be saved by employees on the company server, in the correct folder.

2.3 Customer data must not be stored on employees' local devices such as their laptops or cell phones. Any data downloaded for a work-related purpose should be purged from that device after it is no longer in use.

2.4 Any customer data that is shared with external companies (title, insurance, wholesale lender, etc…) must be encrypted or sent through secure portal.

2.5 Customer data must not be accepted through unencrypted email, MMS message, or other unsecure methods.

2.6 Customer data that is older than 4 years old must be purged immediately. (Optionally you can set a specific interval at which this is done, such as monthly or quarterly)

2.7 Email correspondence containing sensitive data or documents should be purged immediately.

2.8 Physical documents provided by borrowers should be scanned in the office and uploaded directly to the company server.

2.9 Customer data must be encrypted when being stored or transmitted.

3. Password Management Policy

Purpose

Poor password management is one of the top threats facing you and the data you have access to. The Password Policy ensures you take specific steps to improve your password hygiene and eliminate one of the easiest attack vectors for cyber-criminals.

The main purpose of this policy is to provide guidance on password length, complexity, age, and history. This policy is based on guidance from NIST Special Publication 800-63B.

It is highly recommended that employees use a secure password manager to manage their passwords. This allows employees to randomize their passwords and access their accounts without remembering each individual password.

Scope

The Password Policy applies to any employee, contractor, or individual with access to consumer data.

Passwords that are required to be maintained according to the standards within this policy include:

- Device passwords for your work computer (and phone if applicable).
- LOS login passwords
- Wholesale lender passwords
- Email passwords
- Cloud service passwords (Dropbox, Google Drive, etc…)
- Third party provider websites (Appraisal, credit reporting, etc…)
- Any other password that if public could result in unauthorized access to consumer data
- Office/home office network passwords

Policy

3.1 Passwords must be at least 8 characters long. The longer they are, the better. Though 8 characters is the minimum, having passwords with at least 12 characters or more in length makes it exponentially more difficult for your password to be cracked.

3.2 Passwords must not be re-used. Each separate website/account/service must have a unique password. Old passwords should not be re-used.

3.3 Passwords must be comprised of a random combination of upper- and lower-case letters, symbols, and numbers.

3.5 Multi-factor authentication must always be enabled for any account/service that allows it.

3.6 Passwords should not be shared with anyone else. This includes unauthorized employees at your company and employees of third-party companies.

4. Cybersecurity Policy for Employees

Purpose

The purpose of the General Employee Data Security Policy is to set rules that will protect employees, borrowers, and your company from data breaches. The policy points within the Cybersecurity Policy for Employees are wide-ranging and cover multiple attack surfaces.

Scope

The General Employee Data Security Policy applies to any employee, contractor, or individual with access to consumer data.

Policy

This policy will also rely heavily on your edits and customizations to ensure that it covers every aspect of cybersecurity within your organization. If your company takes extra steps to protect borrowers such as vulnerability scans, company assessments, phishing simulations, or anything else, please list that here as well.

4.1 It is the responsibility of each employee to maintain their work devices and follow each policy point.

4.2 All work devices must have at least one active anti-malware program.

4.3 Anti-malware programs on work devices must be updated as soon as updated are released.

4.4 Anti-malware programs on work devices must be configured to automatically check for updates.

4.5 All work devices must be password protected, with passwords that conform to the Password Policy.

4.6 All work devices must be safely stored in a secure location inaccessible to the public when not in use. This includes when these devices are at home, a coworking space, or anywhere else.

4.7 Access to work devices must be restricted to the specific employee that uses each device. This includes restricting access to friends, family members, coworkers, and others.

4.8 All work devices must automatically check for and install firmware updates.

4.9 All work devices must be kept up to date with the latest firmware updates.

4.10 Work devices should be used strictly for work purposes. Applications and programs that are not necessary for work should not be installed or used on these devices.

4.11 Mobile devices used for work should not have any side-loaded apps. Side-loaded apps should be expressly disallowed in the mobile device’s settings.

4.12 Employees must complete the assigned regular data security training modules.

4.13 All employees must make their data available to the company and state regulators when requested to do so.

4.14 Employees must complete a yearly data security assessment. This assessment ensures compliance with individual policy points, and helps raise awareness of each point regularly.

4.15 Employees must use a VPN when teleworking.

4.16 Employees must report any suspicious activity or suspected data breaches to management.

4.17 Employees leaving the company must turn over all borrower documents to the company.