DATA SECURITY & PRIVACY TOOLKIT

Last updated April 2022

NATIONAL ASSOCIATION OF REALTORS®

TABLE OF CONTENTS

INTRODUCTION

Trust is at the heart of the real estate business. In this digital economy, trust has taken on new dimensions that impact how real estate professionals collect, share, and, most importantly, protect the information they use in their businesses. Creating a data security program for your business means implementing and maintaining reasonable safeguards to protect the security, confidentiality, and integrity of data, including proper disposal of the data. A privacy policy is a document that discloses some or all of the ways your business collects, shares, protects, and destroys personal information. Often, a written data security program is an internal document provided to and implemented by employees; whereas a privacy policy is distributed more widely such as on your organization's website.

This Data Security and Privacy Toolkit aims to educate real estate associations, brokers, agents, and multiple listing services about the need for data security and privacy; and to assist them in complying with legal responsibilities. The Toolkit provides information about state laws and pending federal regulations regarding data security and privacy protection that may affect your business. In regards to compliance, the Toolkit includes various checklists of issues to consider when drafting a security program tailored to your business's needs. There is no one-size-fits-all approach to security and compliance, but the NATIONAL ASSOCIATION OF REALTORS® (NAR) aims to provide your real estate business with the tools necessary for developing a program that best suits your business. In addition, the Toolkit contains reference to guidance and sample policies created by government or other organizations. The Federal Trade Commission (FTC) has promoted five key principles for protecting personal information. This Toolkit adheres closely to those key principles, which are further explained and set forth in the FTC publication, "Protecting Personal Information; A Guide for Business."

THE IMPORTANCE OF DATA SECURITY AND PRIVACY

Most real estate businesses – brokerages, associations, and MLSs – keep sensitive, personal information in their files.

Brokers and agents collect personal information for a variety of reasons, including:

- Social Security numbers in order to perform credit checks on renters or to complete a short sale transaction;
- Bank account information and Social Security numbers contained in mortgage documents and closing statements;
- Personal checks given as earnest money;
- Credit card information to make various payments for inspections or appraisals; or
- Drivers' license numbers as a safety precaution when agents leave the office with a new client for the first time.

Often, this personal information is collected because the agent is trying to help a client, but in reality, the agent may be helping himself and his broker to legal risk.

Associations may collect members' credit card or bank account information in relation to payments for educational courses, RPAC contributions, or other goods and services. Also, associations are employers, so they may also collect employees' Social Security numbers and health information.

If personal information falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. State legislatures realized the potential for this harm and have enacted laws to help protect consumers' personal information. Given the cost of a security breach and the potential reputational harm, safeguarding personal information is just plain good business.

KNOW THE LAWS

It is important for you to know the laws regarding data security and privacy that affect your organization. The purpose of most data security regulation is to encourage businesses to protect personal information under their control in order to avoid misappropriation of that information. Some states have enacted laws that require businesses to have a written information security program in place, dispose of personal information that serves no business purpose, and notify individuals when their personal information may have been accessed because of a security breach. Most state and pending federal legislation allow businesses to take a reasonableness approach to implementing a security program by taking into account the particular business's size, scope of business, amount of resources, and nature and quality of data collected or stored.

Currently, there are no federal laws regarding data privacy that specifically apply to real estate associations or brokerages. However, the Gramm-Leach-Bliley Financial Modernization Act applies to businesses that qualify as financial institutions pursuant to the Act.[1] Some associations and brokerages may also be subject to the Identity Theft Red Flags and Address Discrepancy Rules (Red Flags Rules) contained in the Fair and Accurate Credit Transactions Act of 2003 (FACTA).[2] The Red Flags Rules require all creditors, and those that regularly arrange for credit to be provided, to establish policies and procedures to protect against identity theft.

Although a comprehensive federal data security law does not exist right now, several federal bills that address data security and privacy have been proposed and debated in Congress, and legislation may be forthcoming. These bills contain many elements commonly found in existing state laws, so compliance with state laws should be a good step toward compliance with any future federal legislation.

The National Conference of State Legislatures (NCSL) maintains a list of state data security and privacy laws and pending legislation. This website is an extremely helpful resource to determine which states maintain such laws and where those laws are codified. According to NCSL, 35 states, D.C. and Puerto Rico have some type of law regarding the proper disposal of personal information[3] and the FTC has also issued requirements pertaining to the proper disposal of personal information. Additionally, all 50 states, D.C., Puerto Rico, Guam, and the Virgin Islands have laws regarding notification requirements in the event of a security breach.[4] Finally, according to NCSL, at least 25 states have laws addressing data security practices of entities in the private sector. Review the charts on the following pages to see if your state is listed. Also, keep in mind that many state laws, such as Massachusetts, pertain to any business in the country that maintains personal information of a resident of that state. So, it is wise not only to refer to the laws of the state in which your business is located but also the laws of the states where the individuals whose personal information you collect reside.

The various state laws regarding data security have many common elements but some differences as well. For example, each state has its own definition of "personal information."

In Massachusetts, "personal information" is defined as:

> *A Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:*
>
> *(a)Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account…*[5]

[1] *Gramm-Leach-Bliley Financial Modernization Act (P.L. 106-102, 113 Stat. 1338) (1999). This Data Security and Privacy Toolkit was created without reference to the Gramm-Leach-Bliley Financial Modernization Act and should not be relied upon for compliance with that Act.*

[2] *Fair and Accurate Credit Transactions Act of 2003; Pub. Law 108-159 (Dec. 4, 2003); 117 Stat. 1952. To learn more about the Red Flags Rules and how it may affect your organization, check out: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule*

[3] *National Conference of State Legislatures, "Data Disposal Laws," available at: https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.*

[4] *National Conference of State Legislatures, "State Security Breach Notification Laws," available at: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.*

[5] *Standards for the Protection of Personal Information of Residents of the Commonwealth; 201 CMR § 17.02.*

California's definition of "personal information" under its data breach law is different, as it is defined as:

> *(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:*
>
> *(a) Social Security number; (b) driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (c) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;*
>
> *(d) medical information; (e) health insurance information; (f) unique biometric data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual (unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes); (g) information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.*
>
> *(2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.*[6]

The two definitions above may look similar, but their differences are significant. The Massachusetts definition appears broader because it includes even encrypted data elements. Information is encrypted if the data is transformed in a way that its meaning cannot be ascertained or understood without the use of a confidential process or key. Also, in Massachusetts, a financial account number need not be accompanied by a security code or password. In California, the data breach statute would not be triggered if one of the data elements was encrypted and, in order to qualify as "personal information," an account number must be found in combination with a security code or password. However, unlike Massachusetts, the California data breach statute's definition of personal information includes an email username in combination with information that would permit access to an online account.

Even still, the California Consumer Privacy Act ("CCPA"), enacted in 2018 to provide California residents with greater data privacy rights, adopts a different, and expansive, definition of "personal information":

> *Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.*[7]

Unless otherwise noted, for the purpose of this Toolkit, "personal information" will be interpreted broadly to mean any information that can be used to uniquely identify, con- tact, or locate a single person, or can be used with other sources to uniquely identify a single individual. For specific requirements, businesses should consult applicable law and legal counsel.

[6] *Cal. Civ. Code § 1798.82(h).*

[7] *Cal. Civ. Code § 1798.140 (n)(1).*

DATA DISPOSAL LAWS

Personal identifiable information is often collected by businesses and stored in various formats, including electronically and physical copies. With identity theft a growing problem, many states have passed laws that require entities to destroy, dispose, or otherwise make stored personal information unreadable or undecipherable in order to protect an individual's privacy. At least 35 states, and Puerto Rico have laws that govern the disposal of personal data held by a business. Additionally, the FTC issued requirements pertaining to the proper disposal of personal data.

As of August 27, 2021

Alabama
Ala. Code § 8-38-10

Alaska
Alaska Stat. § 45.48.500 et. Seq.

Arizona
Ariz. Rev. Stat. § 44-7601

Arkansas
Ark. Code § 4-110-103, 104

California
Cal. Civ. Code §§ 1798.81, 1798.81.5, 1798.84

Colorado
Colo. Rev. Stat. § 6-1-713

Connecticut
Conn. Gen. Stat. § 42-471

Delaware
Del. Code tit. 6 § 5001C to -5004C, tit. 19 § 736

Florida
Fla. Stat. § 501.171(8)

Georgia
Ga. Code § 10-15-2

Hawaii
Haw. Rev. Stat. §§ 487R-1, 487R-2, 487R-3
Haw. Rev. Stat. § 261-17.7(d)
Haw. Rev. Stat. § 52D-14(c) (2018 S.B. 2738)

Illinois
20 ILCS 450/20
815 ILCS 530/30
815 ILCS 530/40

Indiana
Ind. Code §§ 24-4-14-8, 24-4.9-3-3.5(d)

Kansas
Kan. Stat. § 50-6, 139b(2)

Kentucky
Ky. Rev. Stat. § 365.725

Louisiana
LA. R.S. 51:3074(B)

Massachusetts
Mass. Gen. Laws Ch. 93I, § 2

Maryland
Md. Comm. Law § 14-3502
Md. State Govt. Code §§ 10-1303

Michigan
MCL § 445.72a

Montana
Mont. Code Ann. §30-14-1703

Nebraska
Neb. Rev. Stat. § 87-808(1)

Nevada
Nev. Rev. Stat. § 603A.200

New Jersey
N.J. Stat. § 56:8-161, -162

New Mexico
N.M. Stat. § 57-12C-3

New York
N.Y. Gen. Bus. Law § 399-H

North Carolina
N.C. Gen. Stat. § 75-64

Oregon
Ore. Rev. Stat. § 646A.622

Rhode Island
R.I. Gen. Laws § 6-52-2

South Carolina
S.C. Code § 37-20-190
S.C. Code § 30-2-310

Tennessee
Tenn. Code § 39-14-150(g)

Texas
Tex. Bus. and Com. Code. Ann. § 72.004, § 521.052

Utah
Utah Code § 13-44-201

Vermont
9 Vt. Stat.§ 2445

Virginia
Va. Code § 2.2-2009(F)

Washington
Wash Rev. Code § 19.215.020

Wisconsin
Wisc. Stat. § 134.97

Puerto Rico
2014 Law #234-2014

PLEASE NOTE: The National Conference of State Legislatures serves state legislators and their state. This site provides general comparative information only and should not be relied upon or construed as legal advice.

STATE SECURITY BREACH NOTIFICATION LAWS

All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring that businesses provide notification of security breaches involving personal information.

As of April 15, 2021

Alabama
Ala. Code § 8-38-1 et seq.

Alaska
Alaska Stat. § 45.48.010 et seq.

Arizona
Ariz. Rev. Stat. §18-551 to -552

Arkansas
Ark. Code §§ 4-110-101 et seq.

California
Cal. Civ. Code §§ 1798.29, 1798.82

Colorado
Colo. Rev. Stat. § 6-1-716

Connecticut
Conn. Gen Stat. §§ 36a-701b, 4e-70

Delaware
Del. Code tit. 6, § 12B-101 et seq.

Florida
Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)

Georgia
Ga. Code §§ 10-1-910 to -912; 46-5-214

Hawaii
Haw. Rev. Stat. §487N-1 et seq.

Idaho
Idaho Stat. §§ 28-51-104 to -107

Illinois
815 ILCS §§ 530/1 to 530/25
815 ILCS §530/55 (2020 S.B. 1624)

Indiana
Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.

Iowa
Iowa Code §§ 715C.1, 715C.2

Kansas
Kan. Stat. § 50-7a01 et seq.

Kentucky
KRS § 365.732
KRS §§61.931 to 61.934

Louisiana
La. Rev. Stat. §§ 51:3071 et seq.

Maine
Me. Rev. Stat. tit. 10 § 1346 et seq.

Maryland
Md. Code Com. Law §§ 14-3501 et. Seq
Md. State Govt. Code §§ 10-1301 to -1308

Massachusetts
Mass. Gen. Laws § 93H-1 et seq.

Michigan
Mich. Comp. Laws §§ 445.63, 445.72

Minnesota
Minn. Stat. §§ 325E.61, 325E.64

Mississippi
Miss. Code § 75-24-29

Missouri
Mo. Rev. Stat. § 407.1500

Montana
Mont. Code §§ 2-6-1501 to -1503, 30-14-1704, 33-19-321

Nebraska
Neb. Rev. Stat. §§ 87-801 et seq.

Nevada
Nev. Rev. Stat §§ 603A.010 et seq., 242.183

New Hampshire
N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21

New Jersey
N.J. Stat. § 56:8-161, 163

New Mexico
N.M. Stat. §§ 57-12C-1

New York
N.Y. Gen. Bus. Law § 899-AA

North Carolina
N.C. Gen. Stat §§ 75-61, 75-65, 14-113.20

North Dakota
N.D. Cent. Code §§ 51-30-01 et seq.

Ohio
Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192

Oklahoma
Okla. Stat. §§ 74-3113.1, 24-161 to -166

Oregon
Oregon Rev. Stat. §§ 646A.600 to .628

Pennsylvania
73 Pa. Stat. §§ 2301 et seq.

Rhode Island
R.I. Gen. Laws §§ 11-49.3-1 et seq.

South Carolina
S.C. Code § 39-1-90

South Dakota
S.D. Cod. Laws §§ 20-40-19 to -26

Tennessee
Tenn. Code §§ 47-18-2107; 8-4-119

Texas
Tex. Bus. & Com. Code §§ 521.002, 521.053

Utah
Utah Code §§ 13-44-101 et seq.

Vermont
Vt. Stat. tit. 9 §§ 2430, 2435

Virginia
Va. Code §§ 18.2-186.6, 32.1-127.1:05

Washington
Wash. Rev. Code §§ 19.255.010, 42.56.590

West Virginia
W.V. Code §§ 46A-2A-101 et seq.

Wisconsin
Wis. Stat. § 134.98

Wyoming
Wyo. Stat. § 6-3-901(b), §§ 40-12-501 to -502

District of Columbia
D.C. Code §§ 28-3851 et seq.
D.C. Code § 23-98

Guam
9 GCA §§ 48-10 et seq.

Puerto Rico
10 Laws of Puerto Rico §§ 4051 et seq.

Virgin Islands
V.I. Code tit. 14, §§ 2208, 2209

PLEASE NOTE: The National Conference of State Legislatures serves state legislators and their state. This site provides general comparative information only and should not be relied upon or construed as legal advice.

STATE DATA SECURITY LAWS—PRIVATE SECTOR

At least 25 states and the District of Columbia have enacted laws that address data security practices of entities in the private sector. Under most of these laws, a business that owns, licenses, or maintains personal information about a resident of that state must implement and maintain "reasonable security procedures and practices" pertaining to the personal information collected, stored or used. In determining what constitutes "reasonable security procedures and practices," businesses should consider the nature of the information collected, stored or used, and the means necessary to protect that information from unauthorized access, destruction, use, modification or disclosure. This chart does not include administrative rules and regulations of various states that require businesses to follow certain data security practices (see, e.g., California (Cal. Civ. Code §§ 1798.100-1798.199, California Privacy Rights Act of 2020 (effective January 1, 2023)), Colorado (3 CCR 704-1), Massachusetts (201 Mass. Code of Regs. 17.00-17.04) and New York (23 NYCRR Part 500).

As of May 29, 2019

Alabama
Act No. 2018-396

Arkansas
Ark. Code § 4-110-104(b)

California
Cal. Civ. Code § 1798.81.5
Calif. Civil Code § 1798.91.04

Colorado
Colo. Rev. Stat. § 6-1-713 to -713.5

Connecticut
Conn. Gen. Stat. § 38a-999b
Conn. Gen. Stat. § 4e-70

Delaware
Del. Code § 12B-100

Florida
Fla. Stat. § 501.171(2)

Illinois
815 ILCS 530/45

Indiana
Ind. Code § 24-4.9-3-3.5(c)

Kansas
K.S. § 50-6, 139b

Louisiana
La. Rev. Stat. § 3074 (2018 SB 361)

Maryland
Md. Code Com Law §§ 14-3501 to -3503

Massachusetts
Mass. Gen. Laws Ch. 93H § 2(a)

Minnesota
Minn. Stat. § 325M.05

Nebraska
Neb. Rev. Stat. §§ 87-801-807 (2018 L.B. 757)

Nevada
Nev. Rev. Stat. §§ 603A.210, 603A.215(2)

New Mexico
N.M. Stat. § 57-12C-4 to -5

New York
N.Y. Gen. Bus. Law § 899-BB

Ohio
Ohio Rev. Stat. §1354.01 to 1354.05 (2018 S.B. 220)

Oregon
Or. Rev. Stat. § 646A.622

Rhode Island
R.I. Gen. Laws § 11-49.3-2

South Carolina
S.C. Code § 38-99-10 to -100 (2018 HB 4655)

Texas
Tex. Bus. & Com. Code § 521.052

Utah
Utah Code §§ 13-44-101, -201, -301

Vermont
9 V.S.A. § 2446-2447 (2018 HB 764)

District of Columbia
D.C. Code § 23-98

FTC: FIVE KEY PRINCIPLES TO A SOUND DATA SECURITY PROGRAM

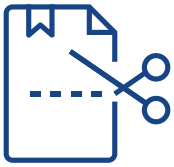
The Federal Trade Commission has set forth the following five key principles for businesses to follow when creating a data security program.[8]

1

TAKE STOCK

Know what personal information you have in your files and on your computers

2



SCALE DOWN

Keep only what you need for your business.

3

LOCK IT

Protect the information that you keep.

4

PITCH IT

Properly dispose of what you no longer need.

5

PLAN AHEAD

Create a plan to respond to security incidents.

[8] *Federal Trade Commission, "Protecting Personal Information; A Guide for Business," available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf*

TAKE STOCK

Perform an information inventory to determine what type of information your business maintains and why; who maintains or has access to the collected information; how the information is collected; and whether a user or consumer may opt-out of your collection of the information. The more thorough your inventory, the better equipped you'll be to create a written data security program that better protects your organization

As part of your information inventory, be sure to talk to information technology staff, human resources, accounting personnel, outside service providers, employees and independent contractors. Association executives and brokers should also inventory all computers, laptops, flash drives, disks, home computers, mobile devices, and other equipment to find out where sensitive data is stored.

INFORMATION INVENTORY CHECKLIST

A complete information inventory should answer the following questions:

WHO SENDS PERSONAL INFORMATION TO YOUR BUSINESS?

- Consumers
- Independent contractors
- Employees/Job applicants
- Members
- Credit card companies
- Banks or other financial institutions
- Brokerages
- Call centers
- Contractors
- Other

HOW DOES YOUR BUSINESS RECEIVE PERSONAL INFORMATION?

- Websites
- Emails
- Mail
- Interviews
- Electronic payment system
- Contractors

WHERE DOES YOUR BUSINESS KEEP THE INFORMATION YOU COLLECT?

- Central computer database
- Individual laptops
- Disks
- File cabinets
- Branch offices
- Employees/Licensees have files at home
- Mobile devices
- Cloud computing service
- Other

WHO HAS ACCESS TO THE INFORMATION?

- Specific employees/licensees
- Vendors
- Independent contractors
- Consumers
- Other

WHAT KIND OF INFORMATION DOES YOUR BUSINESS COLLECT AT EACH ENTRY POINT?

- Individuals' names
- Postal address
- Telephone/fax number
- Email address
- Social Security number
- Driver's license number
- Tax ID
- Passport number
- Real Estate License number
- Other Government-issued identification number
- Credit card or debit card number
- Checking account information
- Security code, access code, or password for an individual's financial account
- Credit history
- Mortgage application
- Medical information
- Health insurance information
- Race/ethnicity
- Religious belief
- Sexual orientation
- Financial information (e.g., balance, history, etc.)
- Precise geolocation information
- Biometric data
- Website user activity
- **Unique persistent identifier** (e.g., customer number, user alias, IP address, etc.)
- **Preference profile** (e.g., a list of information, categories, or information or preferences associated with a specific individual or computer or device)

SCALE DOWN

Once you've performed an information inventory and understand what type of information your business collects and how and why, it's time to consider whether or not you need to continue collecting or retaining such information. Here's the rule:

> *If your association or brokerage does not have a legitimate business need for the personal identifiable information—then don't collect it. If there is a legitimate business need for the information, then keep it only as long as it's necessary. Once that business need is over, then properly dispose of it.*

Specifically, the FTC recommends:

- Use Social Security numbers only for required and lawful purposes–like reporting employee taxes. Don't use Social Security numbers unnecessarily–for example, as an employee or customer identification number, or because you've always done it.
- If your company develops a mobile app, make sure the app accesses only the data and functionality that it needs. And don't collect and retain personal information unless it's integral to your product or service. Remember, if you collect and retain data, you must protect it.
- Don't keep customer credit card information unless you have a business need for it. For example, don't retain the account number and expiration date unless you have an essential business need to do so. Keeping this information–or keeping it longer than necessary–raises the risk that the information could be used to commit fraud or identity theft.
- Scale down access to data. Follow the "principle of least privilege." That means each employee should have access only to those resources needed to do their particular job.[9]

If you must keep information for business reasons or to comply with the law, then develop and adhere to a document retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when you no longer need it. Refer to the tips for creating a Document Retention Policy provided in the section titled "Pitch It."

[9] *https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how*

LOCK IT

Now you've taken stock and know what personal information your organization collects, how it is collected, and why. You've scaled down and know what personal information is necessary for you to continue collecting and what information you can avoid collecting in the future. Now it's time for you to protect the personal information you maintain. The FTC recommends four key elements for your protection plan: physical security, electronic security, employee training, and the security practices of contractors and service providers.

CHECKLIST FOR PROTECTING PERSONAL INFORMATION

The following checklist contains tips and recommendations for protecting personal information. For more guidance on protecting personal information, check out the FTC's Protecting Personal Information, a Guide for Business.

PHYSICAL SECURITY

- Store paper documents and tangible files containing personally identifiable information in a locked room or in a locked file cabinet.
- Limit access to employees with a legitimate business need.
- Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- If you maintain offsite storage facilities, limit employee access to those with a legitimate business need.

ELECTRONIC SECURITY

- Identify the computers or servers where personally identifiable information is stored.
- Identify all connections to those computers. For example, the internet, electronic cash register, computers at branch offices, computers used by service providers to support your network, and wireless devices.
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
- Don't store personally identifiable information on any computer with an internet connection unless it's essential for conducting your business.
- Encrypt sensitive information that you send to third parties over public networks.
- Regularly run up-to-date antivirus and antispyware programs on individual computers and on servers on your network.
- When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.
- Pay particular attention to the security of your web applications such as the software used to retrieve information from visitors to your website.
- Routinely check websites, such as us-cert.gov, and your cybersecurity vendors' websites for notifications regarding new vulnerabilities.
- Require the use of a token, smart card, thumb print, or other biometric—as well as a password—to access a computer that contains personal information.
- Restrict employees' ability to download unauthorized software.
- Instruct employees not to share sensitive personal information, such as Social Security numbers, via email.

PASSWORD MANAGEMENT

- Require employees to use strong passwords, using a combination of letters, numbers, and characters, as well as multi-factor authentication.
- Prohibit sharing or posting passwords.
- Use password-activated screen saves to lock employee computers after a period of inactivity.
- When installing new software, immediately change vendor-supplied default passwords to a more secure, strong password.
- Warn employees about social engineering. For example, alert them to possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.
- Consider using a password vault to store all your passwords.
- Advise employees against using the same password for multiple platforms since a breach of one platform will allow the login to all other platforms that share the same password.

MOBILE DEVICE SECURITY

- Assess whether personal information really needs to be stored on a laptop. If not, wipe it out.
- Consider prohibiting the storage of personal information on laptops.
- If a laptop contains personal information, encrypt it and configure it so users can't download any software or change the security settings without approval from your IT specialist.
- Train employees to be mindful of security when they're on the road.
- Consider using mobile device management (MDM) tools which will enable the remote management of all your mobile assets including location services and the remote wipe of mobile assets in case of any cybersecurity compromise.
- Turn off the Bluetooth when it's not in use – cyber criminals can pair with your mobile device through the Bluetooth connection and steal personal information.
- Backup your files – to avoid losing access to your information if a mobile device is stolen, make automated backups.

FIREWALLS

- Use a firewall to protect your computer from hacker attacks while it is connected to the internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.
- Determine whether you need a firewall to separate your network from the internet.
- Set access controls – settings that determine who gets through the firewall and what they will be allowed to see – to allow only trusted employees with a legitimate business need to access the network.
- Implement additional firewalls to protect computers that store personal identifiable information.

WIRELESS AND REMOTE ACCESS

- Determine if you use wireless devices like cell phones to connect to your computer network or to transmit personal information. Limit the devices that can use a wireless connection to access your computer network.
- Encrypt information you send via your wireless network to prevent neighboring networks from accessing the information.
- Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.
- Unless there are proper cybersecurity measures in place (e.g., VPN), do not use public Wi-Fi and use your cellular connection instead.

DIGITAL COPIERS

- Set your copier to overwrite the hard drive as frequently as feasible, at least once a month
- All copiers that were used to process sensitive information should be properly disposed in which it is sanitized of all data saved in its data storage.

DETECTING BREACHES

- Consider using an intrusion detection system to quickly detect network breaches when they occur.
- Maintain a central log of security-related information to monitor activity on your network so that you can spot and timely respond to any attacks.
- Monitor incoming and outgoing traffic for signs that someone is trying to hack in.
- Develop and implement a breach response plan.

STAFF TRAINING

- Check references or do background checks before hiring employees and independent contractors who will have access to personal data.
- Conduct training on your data security program, including how to spot security vulnerabilities and potential disciplinary measures for violations of the policy.
- Make sure employees and independent contractors understand the importance of abiding by your company's data security program.
- Require employees and independent contractors to notify you immediately if there is a potential security breach, such as a lost or stolen laptop or a downloaded virus.
- Know which and limit the employees and independent contractors with access to personal information.
- Create a procedure for terminating an employee or independent contractor's access to personal information when they leave the company.
- Inform employees and independent contractors of your company's confidentiality policies.
- Teach your employees and independent contractors about the dangers of phishing such as unknown or suspicious links or phone calls.

SECURITY PRACTICES OF CONTRACTORS AND SERVICE PROVIDERS

- Before you outsource any of your business functions–payroll, web hosting, customer call center operations, cloud computing, or the like–investigate the company's data security practices and make sure they follow industry standards and best practices.
- Require service providers to adhere to specific security expectations in any service contracts.
- Insist that service providers provide notice of any security incidents, even if the incident did not lead to an actual compromise of data.
- Insist that contractors and service providers adhere to all applicable federal and state laws regarding data security and privacy.

PITCH IT

According to the FTC and many state laws, proper disposal of personal information is an important step in any data security program. Implementation of a Document Retention Policy that is reasonable and appropriate will help prevent unauthorized access to personal information. But the question remains: What constitutes "proper disposal"? In general, personal information is properly disposed if it cannot be read or reconstructed. The FTC recommends that a business burn, shred, or pulverize paper records and use wipe utility programs or otherwise destroy electronic records. Simply deleting files from the computer using the keyboard or mouse commands usually isn't suffcient. Also, make sure employees who work from home follow the same procedures for the disposal of personal information.

Like all data security policies, there is no "one-size-fits-all" model for document retention. NAR has issued guidance for association record retention and brokerage record retention The following checklist provides a brief description of the process an association or brokerage should undertake in creating a document retention policy. Following that is a list of different types of documents and some recommended time frames for how long the association should maintain these records.

This checklist and the guidance are not intended to be comprehensive or even authoritative; rather, they are intended to serve as a guide for associations and brokerages in creating their own policies. State law will determine how long an organization needs to maintain its records. Remember, a document retention policy adopted and followed by the association or brokerage will likely reduce the costs and burdens of any future litigation.

CHECKLIST FOR A DOCUMENT RETENTION POLICY

A. PROCESS FOR CREATING A DOCUMENT RETENTION POLICY

IDENTIFY SOURCES AND TYPES OF INFORMATION

- Gather together the employees who are familiar with the documents and other information your business maintains. Depending on the size of the organization, the number of individuals could vary. A person familiar with how the business maintains electronic information should attend the meeting. Please refer to the "Take Stock" section regarding information inventory for more information and guidance for completing this step.

IDENTIFY AND DOCUMENT CURRENT RETENTION POLICIES

- Determine what policies (if any) are currently governing your organization's document retention policies and reduce those to writing, including its policies for retaining electronic information.

EVALUATE EXISTING POLICIES

- Decide whether your organization's current policies are adequate or whether a new policy is necessary.

CREATE A POLICY (IF NECESSARY)

The document retention policy should include the following:

- How long certain documents should be retained
- Policy's effective date and date of last review
- Individual responsible for the policy
- Purpose of the policy
- **Definitions** (if needed)
- Process for preserving records if litigation arises or is likely

LEGAL REVIEW OF DOCUMENT RETENTION POLICY

- Consult legal counsel during the creation and finalization of the policy.

DISTRIBUTE THE POLICY TO EMPLOYEES AND INDEPENDENT CONTRACTORS AND ENSURE ADHERENCE TO THE POLICY

- This is the most important step! Having a policy that isn't followed may actually be worse than not having any policy if litigation arises.

PERIODICALLY REVIEW THE POLICY

- Review the policy on an ongoing basis to be sure the policy adheres to relevant laws and meets business needs.

B. ITEMS TO CONSIDER FOR A DOCUMENT RETENTION POLICY

A few items are listed below:

FORMAT USED TO MAINTAIN DOCUMENTS

- Generally, there are no requirements on the type of format that must be used to maintain documents and other information. When the hard-copy originals are not legally necessary, reducing paper documents to an electronic format may be advantageous because it will save physical space. Note, however, that an increase of electronic storage could also increase discovery cost and exposure if litigation arises.

PRIVACY CONSIDERATIONS AND PROPER DOCUMENT DESTRUCTION

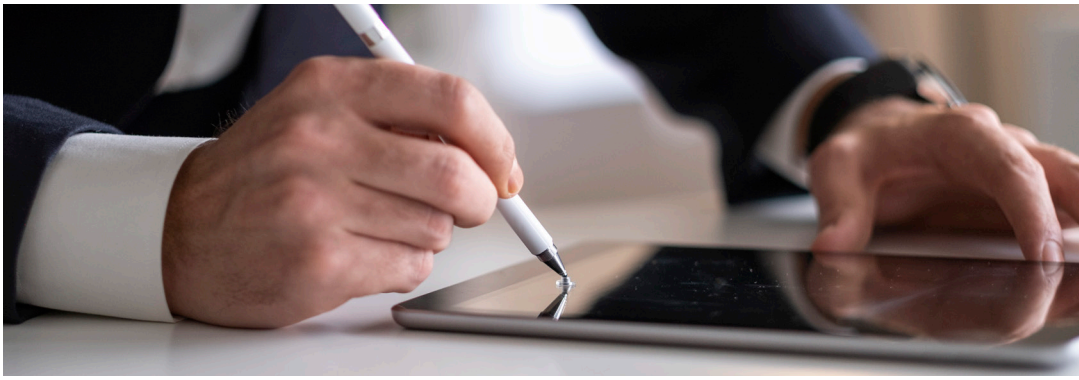
- Certain types of records, such as employment records, are governed by state or federal privacy laws. Therefore, you must be familiar with those laws and also any rules or other restrictions governing the destruction of these documents.

OTHER LEGAL CONSIDERATIONS

- The legal requirements for retention of certain documents will vary based on a variety of factors. For example, employment statutes may only apply to employers with a minimum numbers of employees, and the IRS audits are generally initiated within three years, but the IRS can audit a return seven years later if negligence was involved and indefinitely in cases of tax fraud. Each company must be aware of the laws that apply to their situation

C. DOCUMENT RETENTION PERIODS

Below is a list of types of documents that you may maintain in their files. Next to each entry are some suggested time periods for which the organization should maintain these documents. These are conservative estimates and do not prevent any organization from extending these time periods beyond these minimums. These requirements vary by state, and so you will need to consult with your attorney when creating the policy, as stated above.



ACCOUNTING RECORDS

- **Accounts payable** (seven years)
- **Accounts receivable** (seven years)
- **Annual financial statements** (permanent)
- **Bank statements** (seven years)
- **Bank reconciliations** (seven years)
- **Canceled checks: routine matters** (seven years)
- **Canceled checks: special** (loan repayment, etc.) (permanent)
- **Correspondence: routine** (four years)
- **Deeds and closing papers** (permanent)
- **Deposit slips** (four years)
- **Electronic payment records** (seven years)
- **Employee expense reports** (seven years)
- **Fixed-asset acquisition invoices** (after disposal) (seven years)
- **Freight bills** (seven years)
- **General ledgers** (permanent)
- **Income tax returns** (permanent)
- **Inventory count and costing sheets** (seven years)
- **Insurance policies** (after expiration) (four years)
- **Investments** (after disposal) (seven years)
- **Mortgages, loans and leases** (paid) (seven years)
- **Payroll journals and ledgers** (permanent)
- **Purchase orders** (except accounts payable copy) (one year)
- **Purchase invoices and orders** (seven years)
- **Receiving sheets** (two years)
- **Sales commission reports** (five years)
- **Sales records** (seven years)
- **Sales tax returns and exemption support** (five years)
- **Subsidiary ledgers** (seven years)
- **Tax returns** (federal and state) (if applicable) (permanent)

ASSOCIATION CORPORATE RECORDS

- **Articles of Incorporation and amendments** (permanent)
- **Bylaws and amendments** (permanent)
- **Corporate filings** (permanent)
- **Corporate minute book** (permanent)
- **IRS exemption letter** (permanent)

ELECTRONICALLY STORED INFORMATION

- **Specific documents in electronic formats will be treated according to the timeframes set forth elsewhere in the policy. The policy should state how long an organization maintains information stored on its backup tapes and other backup systems. The policy should also state that the purpose of the backups is to restore the business's computer network in the event of a crash.**

EMPLOYMENT RECORDS

- **Documents relating to job recruitment: advertising, job orders submitted to employment agencies, interviewing, testing, hiring, training, demotions, promotions, layoffs, discharge, and other personnel decisions** (one year)
- **Employee benefit plan documents** (duration of plan)
- **FMLA leave records including: all FMLA information and notices distributed to these employees and records of any FMLA disputes** (duration of employment plus ten years)
- **Garnishments/wage assignments** (three years)
- **Immigration I-9 forms** (duration of employment plus one year, minimum of three years)
- **Medical records relating to the exposure of the employee to any toxic or hazardous substances** (duration of employment plus 30 years)
- **Payroll records showing name, address, date of birth, occupation, rate of pay, and weekly compensation** (three years)
- **Personnel records** (ten years after employment ends)
- **Record of all occupational injuries, including those under state workers compensation law and any ERISA awards** (five years for ERISA; state law requirements will vary)

LEGAL DOCUMENTS

- **Contracts** (ten years after expiration)
- **License applications** (one year after expiration)
- **Licenses** (one year after expiration)
- **Trademarks, patents and copyrights** (permanent)
- **Warranties and guaranties** (two years beyond terms of the warranty)
- **Correspondence: legal** (permanent)

MLS DOCUMENTS

- **Rules and regulations** (permanent)
- **MLS policies** (permanent)
- **Listing agreements** (at least until expiration of listing)
- **Sold property information** (at least ten years)
- **Lockbox key agreements/leases** (one year after agreement terminates)
- **MLS service mark license agreements** (permanent)
- **Contracts** (ten years after expiration)
- **Subscription agreements** (ten years after expiration)
- **Participation agreements** (ten years after expiration)
- **Website click-through confirmations** (ten years)

ASSOCIATION DOCUMENTS

- **Association charter** (permanent)
- **Territorial jurisdiction** (permanent)
- **Member file and membership applications** (two years after membership terminates, with Social Security number and other financial information removed [if applicable])
- **Professional standards hearing records: ethics** (result of hearing—permanent; rest of hearing file—minimum of one year after satisfaction of sanctions [if any] and there is no threat of litigation)
- **Arbitration/mediation** (minimum of one year after payment of award [if any] and there is no threat of litigation)

PROPERTY RECORDS

- **Deeds of title** (permanent)
- **Leases** (two years after expiration)
- **Depreciation schedules** (permanent)
- **Property damage** (seven years)
- **Property tax** (permanent)
- **Appraisals** (permanent)
- **Blueprints/plans** (permanent)
- **Warranties and guaranties** (two years beyond terms of the warranty)

PENSION AND PROFIT SHARING

- **ERISA disclosure documents** (six years from date disclosure was due)
- **IRS determination letter(s)** (permanent)
- **Forms 5500 and plan documents** (permanent)

PLAN AHEAD

As explained in the Introduction, currently many states have laws that require a business to keep personal information secure and all states have laws that require a business to notify individuals in the event that security is breached. Therefore, it is advisable and may be necessary to have a written data security program in place and a policy that addresses what to do in the event of a breach. Remember, your organization may be subject to the laws of multiple states if it collects personal information from residents of multiple states. So, it is important to know which laws you must adhere to.

Although each state data security and breach notification law is different, they contain some common elements. For example, many laws require businesses to designate an employee to coordinate and implement the data security and breach notification program. Such laws also set forth the definition of "personal information" and the requirements of breach notification, such as who must receive notification and the timing, format, and content of such notification. Most laws also include provisions regarding a business's liability for failure to comply, and provide a private right of action to allow individuals to sue businesses for actual damages that result from not receiving timely notice of the data breach.

This section of the Toolkit provides information to help in the implementation of your own written data security program and includes the following:

- Checklist for implementing a data security program
- Model written data security program created by the Massachusetts Association of REALTORS®
- Checklist for responding to a data security breach

For additional guidance, check out the sample written security program and checklist created by the Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation.[10]

Please remember that the information contained herein is not intended to be comprehensive or even authoritative; rather, it is intended to serve as a guide for real estate businesses in creating their own policies.

[10] *Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation, "A Small Business Guide: Formulating a Comprehensive Written Information Security Program," available at: paulohm.com/classes/infopriv13/files/week13/MA%20form%20WISP.pdf; and "201 CMR 17.00 Compliance Checklist," available at: mass.gov/doc/201-cmr-1700-compliance-checklist-0/download.*

CHECKLIST FOR IMPLEMENTING A DATA SECURITY PROGRAM

Designate one or more employees to maintain the data security program.

Understand and describe in writing your organization's current safeguards for limiting risks to the security or integrity of any personal information including but not limited to:

- Ongoing employee training
- Employee compliance with policies and procedures
- Means for detecting and preventing security system failures
- Implement reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas, or containers
- Implement reasonable restrictions upon how personal information is stored, accessed, and transported by employees and independent contractors outside of business premises, including electronically
- Impose disciplinary measures for violations of the data security program
- Prevent terminated employees from accessing records containing personal information
- Oversee service providers by:
  - Choosing service providers carefully
  - Requiring third-party service providers by contract to implement and maintain such appropriate security measures for personal information
- Regularly monitor the effectiveness of the data security program and upgrade information safeguards as necessary to limit risks
- Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information
- Document responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information
- Provide for secure user authentication protocols and access control measures
- Encrypt all transmitted records and files containing personal information that will travel across public networks, be transmitted wirelessly, or are stored on laptops or other portable devices
- Implement reasonable monitoring of systems for unauthorized use of or access to personal information
- If applicable, install reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information
- Maintain reasonably up-to-date versions of system security agent software
- Educate and train employees and independent contractors on the proper use of the computer security system and the importance of personal information security

MODEL WRITTEN DATA SECURITY PROGRAM

The following model written data security program was created by the Massachusetts Association of REALTORS® and is included in this Toolkit with the Association's permission. This sample policy is provided as a guide to aid in the development of a written data security program tailored to fit your organization's business needs.

COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM ("WISP")

SECTION 1. PURPOSE AND OBJECTIVE:

MAR's objective, in the development and implementation of this WISP, is to create effective administrative, technical, and physical safeguards for the protection of Personal Information of residents of the Commonwealth of Massachusetts, and to comply with obligations under 201 CMR 17.00 effective March 1, 2010. This WISP sets forth MAR's procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Personal Information of residents of the Commonwealth.

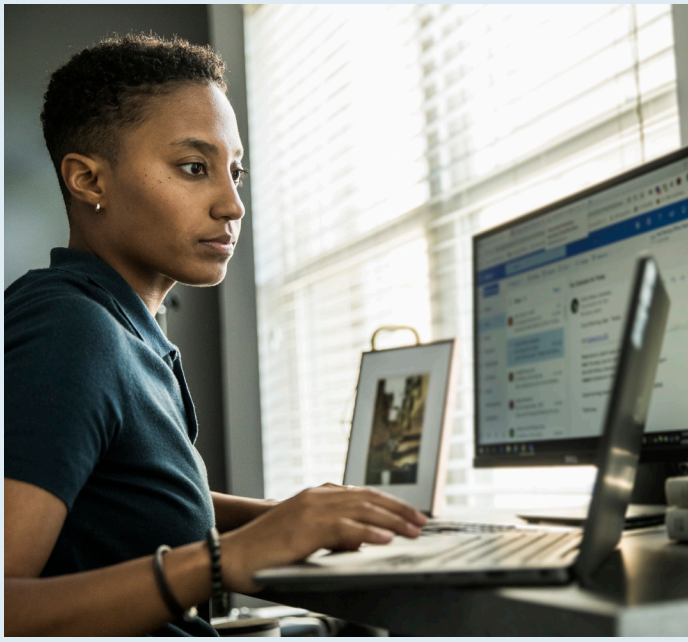
For purposes of this WISP, "Personal Information" as defined by 201 CMR 17.02 means a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal Information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

The purpose of the WISP is, consistent with MGL Ch. 93H Sec. 2 (a) and 201 CMR 17.01, to (a) Ensure the security and confidentiality of Personal Information; (b) Protect against any anticipated threats or hazards to the security or integrity of such information; (c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

SECTION 2. SCOPE OF WISP

This WISP specifically seeks to protect Personal Information by:

1. Identifying reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information;
2. Assessing the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Information;
3. Evaluating the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. Designing and implementing a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and
5. Regularly monitoring the effectiveness of those safeguards.



SECTION 3. DATA SECURITY COORDINATOR:

We have designated the General Counsel to implement, supervise and maintain MAR's WISP. That designated employee (the "Data Security Coordinator") will be responsible for:

A. Initial implementation of the WISP;

B. Training employees;

C. Regular testing of the WISP's safeguards;

D. Evaluating the ability of each of MAR's third-party service providers, to implement and maintain appropriate security measures for the Personal Information to which we have permitted them access, consistent with 201 CMR 17.00; and requiring such third-party service providers by contract to implement and maintain appropriate security measures.

E. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in MAR's business practices that may implicate the security or integrity of records containing Personal Information.

F. Conducting an annual training session for all employees who have access to Personal Information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with MAR's requirements for ensuring the protection of Personal Information.

SECTION 4. INTERNAL RISKS:

As part of its regular business actions and in providing services to its members, MAR needs to collect Personal Information as defined by 201 CMR 17.00. MAR recognizes the sensitivity of this information and the need to protect this information, and as such, seeks to limit the amount of Personal Information that is collected. In all cases Personal Information will be collected only in those instances where it is deemed necessary to carry on the business, services and functions of MAR. MAR recognizes that Personal Information, as defined in 201 CMR 17.00 is regularly collected in the areas identified below. MAR shall take consistent steps to ensure that such information is adequately protected.

1. Employee Records

All records containing Personal Information of employees of MAR shall be maintained by the CEO. Files shall always be restricted electronically, and physical records maintained in a locked file cabinet.

2. Educational Courses, Conferences, and Programs

MAR regularly hosts professional education and conferences for members. Payment for such programs is typically made via credit card or debit card. Information received via the MAR website shall be processed daily and immediately deleted from the MAR website. All electronic records of said Personal Information shall be deleted upon printing. All hard copies of records shall be maintained in locked filing cabinets with limited access for a period of one year. After this period, any hardcopy records shall be destroyed by shredding.

MAR hosts various conferences on an annual basis. As a part of such programs, MAR sells sponsorships to various venders and exhibitors in the Commonwealth. Payment for such services is typically made via credit card. All paper copies of records shall be maintained in locked filing cabinets with limited access for a period determined by the Data Security Coordinator.

3. Product Mall

MAR regularly sells goods to members and non-members of the Association, including for example, books, apparel, Realtor® paraphernalia, real estate forms, brochures etc. When items are purchased with a personal check containing a bank account number, a credit card or debit card, Personal Information will be collected.

Information received via the MAR website or via email shall be processed daily and immediately deleted from the MAR website. All electronic record of said Personal Information shall be deleted upon printed. All paper copies of records (including personal check, credit card or debit card) shall be maintained in locked filing cabinets with limited access for a period determined by the Data Security Coordinator.

4. **REALTOR® Political Action Committee (RPAC)**
   MAR collects contributions from members and affiliates for its Political Action Committee (RPAC). MAR also engages in joint fundraising for RPAC and the National Association of REALTORS Political Action Committee (NAR PAC) and Political Advocacy Fund (NAR PAF). When a personal contribution is collected by MAR, Personal Information is, in most cases, collected. Personal Information is collected when contributions are collected via personal check, credit card or debit card.

   Contributions made by personal check shall be deposited into MAR's bank account on a weekly basis. Checks shall be kept in a locked drawer of the appropriate staff person upon receipt of such contributions. This drawer shall always remain locked when not in use and access shall only be provided to employees depositing and recording such contributions. Copies of all personal checks shall be kept pursuant to the Massachusetts Office of Campaign Finance regulations 970 CMR 1.10(2)(c). All copies shall be kept in a locked filing cabinet with limited access.

   Contributions made via credit card or debit card shall be processed on a weekly basis. Copies of such contributions shall be maintained pursuant to the Massachusetts Office of Campaign Finance regulations 970 CMR 1.10(2)(c). All copies shall be kept in a locked filing cabinet with limited access.

   Personal Information regarding contributions shall not be kept in an electronic manner. Contributions received via the MAR website shall be processed as detailed above and any electronic record of said contribution containing personal information shall be deleted upon printing for record keeping purposes.

5. **Charitable Foundation**
   MAR collects contributions from members and affiliates for its Charitable Foundation. Contributions made by personal check shall be deposited into MAR's bank account on a weekly basis. Checks shall be kept in a locked drawer of the appropriate staff person upon receipt of such contributions. This drawer shall always remain locked when not in use and access shall only be provided to employees depositing and recording such contributions. Personal Information regarding contributions shall not be kept in an electronic manner. All copies and records shall be kept in a locked filing cabinet with limited access.

SECTION 5. INTERNAL SECURITY PROTOCOLS:

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures shall be implemented by MAR. To the extent that any of these measures require a phase-in period, such phase-in shall be completed on or before March 1, 2010:

1. A copy of this WISP shall be distributed to each employee who shall, upon receipt of the WISP, acknowledge in writing that he/she has received and read a copy of the WISP.
2. There shall be immediate retraining of employees on the detailed provisions of the WISP. Any new employees hired after March 1, 2010 shall be notified of MAR's WISP, provided with a copy, and shall be trained on the details of this WISP. All such employees shall acknowledge, in writing, receipt of the WISP.
3. The amount of Personal Information collected by MAR shall be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to comply with other state or federal regulations.
4. Access to records containing Personal Information shall be limited to those persons who are reasonably required to know such information to accomplish your legitimate business purpose or to enable us to comply with other state or federal regulations.
5. All security measures shall be reviewed at least annually, or whenever there is a material change in MAR's business practices that may reasonably implicate the security or integrity of records containing Personal Information. The Data Security Coordinator shall be responsible for this review and shall fully apprise MAR Chief Executive Officer of the results of that review and any recommendations for improved security arising out of that review.
6. Terminated employees must return all records containing Personal Information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

7. A terminated employee's physical and electronic access to Personal Information shall be immediately blocked. Such terminated employee shall be required to surrender all keys to MAR's offices. Moreover, such terminated employee's remote electronic access to Personal Information shall be disabled; his/her voicemail access, e-mail access, internet access, and passwords shall be invalidated. The Data Security Coordinator in conjunction with the Chief Executive Officer shall maintain a highly secured master list of all passwords and keys.
8. Employees must report any suspicious or unauthorized use of customer information to the Data Security Coordinator.
9. Whenever there is an incident that requires notification under M.G.L. c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of Personal Information for which MAR is responsible.
10. Employees are prohibited from keeping open files containing Personal Information on their screen when they are not at their desks.
11. At the end of the workday, all files and other records containing Personal Information must be secured in a manner that is consistent with the WISP's rules for protecting the security of Personal Information.
12. Access to electronically stored Personal Information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for a period of 20 minutes at most.
13. Paper or electronic records (including records stored on hard drives or other electronic media) containing Personal Information shall be disposed of only in a manner that complies with M.G.L. c. 93I. MAR shall maintain a paper shredder (or contract for the services of a professional third-party shredding service) on the premises to destroy all paper records containing Personal Information that are no longer needed.
14. Attempted access to user identification after multiple unsuccessful attempts to gain access must be blocked.
15. All corporate owned devices are enrolled with Mobile Device Management (MDM) to enforce security policies and provide remote administration capabilities to the IT team.
16. Additionally, MAR is authorized to remotely wipe corporate data from any MAR owned or personal devices when deemed necessary. Examples include employee termination, a lost mobile device, etc.
17. Access to Personal Information shall be restricted to active user accounts only.

SECTION 6. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are in place:

1. MAR shall always maintain an up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Personal Information, installed on all systems processing Personal Information.
    a. Operating system patches and software firewalls are maintained by Microsoft Endpoint Manager policies.
    b. The firewall in the MAR office will be replaced in the coming months with a device that is automatically patched at regular intervals of time.
2. MAR shall, at all times, maintain an up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing Personal Information.
    a. Microsoft Defender for Endpoint is configured on all devices. This provides centralized reporting and monitoring for all threats.
    b. Sophos antivirus is installed on all macOS devices due to limited functionality of Microsoft Defender on Mac. This is managed by iCorps.

3. All data stored on laptops or other portable devices shall be encrypted, as well as all records and files transmitted across public networks or wirelessly, to the extent technically feasible.
    a. Device management policies are in place to enforce disk encryption on all Windows and macOS devices.
4. All computer systems must be monitored for unauthorized use of or access to Personal Information.
    a. Data Loss Prevention (DLP) policies are in place to detect and alert when PII is shared outside of the organization.
5. There shall be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location.
    a. User IDs and other identifiers are managed in Microsoft 365 admin center.
    b. Microsoft sets a password policy to all accounts based on current best practices.
    c. Additionally, Multi-Factor Authentication (MFA) is in place to help protect against unauthorized account access.
6. Access to the corporate wireless network requires username and password authentication, which is enforced by the Meraki cloud.
    a. Access to Wi-Fi is terminated once employment with the company ceases.

DATA SECURITY BREACH NOTIFICATION

As previously mentioned, every state, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands has a law making it mandatory for a business to provide notice to interested parties when that business has experienced a security breach. In many cases, these laws include requirements regarding the means, content, and timing of the notification. They also specify what constitutes a security breach and what actions a business may be required to take following a breach. Although the laws vary, many are similar in that they require the following elements to be included in the content of a breach notification:

- Description of what happened (unless limited by applicable law)
- Type of protected data involved
- Actions to protect data from further unauthorized access
- What the company will do to assist affected persons
- What affected persons can do to assist themselves
- Contact information for company inquiry response system
- Contact information for local and federal government authorities

When a security breach occurs, there is a lot to do and there may not be much time to craft a notification letter from scratch. That is why it is a good idea to develop a model notice template that can be tailored easily to include the particulars of the incident. Please remember that the content of your notice will be governed by the laws of the various states in which the affected parties reside, and each of those laws should be consulted when drafting your own model template.

CHECKLIST FOR DRAFTING A BREACH NOTIFICATION POLICY

The following checklist presents issues you should consider—and perhaps address—in your business's breach notification policy and potential solutions to those issues.

INDIVIDUAL OR INDIVIDUALS RESPONSIBLE FOR RESPONDING TO A SECURITY BREACH

- Information technology systems employee
- Human resources employee
- Legal counsel
- Public communications/media relations employee
- A security breach response team that includes representatives from more than one department

ACTION UPON LEARNING OR BEING NOTIFIED OF A SECURITY BREACH

- Immediately investigate the incident
- Isolate all affected systems to limit further data loss
- Contact the individual or team responsible for responding to the breach
- Determine whether law enforcement should be notified

INFORMATION TO BE COLLECTED RELATED TO THE BREACH

- Date, time, duration, and location of breach
- How the breach was discovered, who discovered the breach, and any known details surrounding the breach, for example:
- Method of intrusion
- Entry or exit points
- Paths taken
- Compromised systems
- Whether data was deleted, modified and/or viewed
- Whether any physical assets are missing

DETAILS ABOUT THE COMPROMISED DATA:

A list of affected individuals and type

- Data fields
- Number of records affected
- Whether any data was encrypted (if so, which fields)
- What personal information has been compromised
- Determine whether special consultants are necessary to capture relevant information and perform forensics analysis.

IMPLICATIONS OF THE BREACH

- Consider whether other systems are under a threat of immediate or future danger
- Determine whether you are legally obligated to provide notification about the breach and to whom
- Residents of your state
- Residents of other states
- State agencies
- Law enforcement
- Credit reporting agencies
- Determine whether you are contractually obligated to provide notification about the breach
- Consult legal counsel regarding liability, litigation risk, law enforcement investigations, and other legal concerns

PROCEDURES TO BE FOLLOWED IN THE EVENT THAT WRITTEN NOTIFICATION IS REQUIRED OR ELECTED

- Prepare a list of persons to be notified
- Choose a mode of communication for notification, if not already mandated by law
- Draft a notice that complies with applicable laws and contractual obligations
- Consider whether to offer certain remediation services to assist affected persons
- Be sure to comply with any legal or contractual timing requirements

ACTION FOLLOWING A BREACH AND NOTIFICATION

- Prepare an online FAQ and document inquiries and responses
- Review information technology systems and physical security
- Assess operational controls and consider revising company policies or procedures regarding data collection, retention, or storage
- Assess the need for additional employee training in data protection policies and processes
- Review agreements and policies to determine whether any updates or modifications need to be made, including agreements with third parties that handle personal information, website privacy notices and terms of service, agreements with customers or other third parties, and employee handbooks and policies
- Evaluate your response to the breach

PRIVACY POLICY

As stated in the Introduction, a privacy policy is a document that discloses the ways your business collects, shares, protects, and destroys personal information. Often, the privacy policy is made available on a business's website; although that practice is only required for certain types of businesses. Currently, federal privacy laws pertain only to the following types of businesses: those that knowingly collect information about children under the age of 13; those that collect, use, or share an individual's financial information; or provide or use information related to health care services . However, some states, such as California, require certain for-profit entities that collect personal information of California residents to conspicuously post a privacy policy on the website, as well as a link titled "Do Not Sell My Personal Information" to enable residents to opt-out of the sale of their personal information collected by a business to a third party.[11]

Even though no comprehensive federal regulation currently exists that specifically applies to real estate associations or brokerages, several relevant bills have been introduced by Congress and may be adopted in the near future. These bills pertain not only to the online collection of information but online collection as well. And, if your business collects information from a resident of a state with laws requiring privacy policies, such as California, then it is a good idea to have a Privacy Policy in place and to provide a link to that Privacy Policy on each page of your website. This section of the Toolkit will provide a checklist of issues to consider and potentially address when drafting a privacy policy that fits your business needs and some possible solutions to those issues. A copy of NAR's Privacy Policy is also included for guidance.

[11] *California Consumer Privacy Act of 2018 [1798.100–1798.199.100]*

CHECKLIST FOR DRAFTING A WEBSITE PRIVACY POLICY

The following checklist presents issues you should consider—and perhaps address—in your business's privacy policy and potential solutions to those issues.

HOW NOTICE IS PROVIDED TO CONSUMERS

- Clear and conspicuous
- Accessible through a direct link from each page of the website
- May be amended with notice (including a clickwrap agreement)

TYPE OF INFORMATION THAT IS COLLECTED ABOUT A USER

- Information volunteered by the user
- Domain name or IP address
- Type of browser or operating system being used
- Date and time of visit
- Statistical information about which web pages a user visits
- Websites the user visited prior to coming to your website
- Websites the user visits after leaving your website
- Minors are prohibited from volunteering any personal information

HOW THE INFORMATION IS COLLECTED

- Volunteered by the user
- Cookies or other automatic collection of information
- Why the information is being collected
- To improve the content of your website
- To help you understand how people are using your services
- Send notices to the user of updates to the website or new products
- Shared with affiliates, other third parties

WHAT HAPPENS TO THE INFORMATION COLLECTED

- Explain how the information is stored
- Data retention/disposal policy

USER'S ABILITY TO OBTAIN ACCESS TO THE COLLECTED INFORMATION

- Describe under what circumstances the user may access his/her information
- The user may contact you with inquiries or complaints regarding the handling of collected information
- The user may opt-out of collection or sale of the information
- Identity and contact information of the website operator
- Effective date of the privacy policy

MODEL PRIVACY POLICIES

The following privacy policy was created by the NATIONAL ASSOCIATION OF REALTORS® and is maintained on NAR.realtor. This policy is intended to provide an example for developing a privacy policy tailored to your business's specific circumstances. Please be advised that NAR is not subject to the CCPA and those obligations are not addressed in NAR's privacy policy.

NAR.REALTOR PRIVACY POLICY

Updated 04/05/2017

This privacy policy was created by the NATIONAL ASSOCIATION OF REALTORS® and is maintained on NAR.realtor. This policy is intended to provide an example for developing a privacy policy tailored to your business' specific circumstances. Please be advised that NAR is not subject to the CCPA and those obligations are not addressed in NAR's privacy policy.

We recognize the importance of protecting the personal information you provide at websites owned or controlled by the NATIONAL ASSOCIATION OF REALTORS® (NAR). One of NAR's sites, REALTOR.com, has posted its own "privacy polices" and "terms of use." For the rest of NAR's websites, we maintain the following privacy policy:

1. **NAR gathers the following types of information needed to process your transactions, fulfill your requests, and maintain our membership records:**
   - **Contact information you provide** (for example, your personal and business addresses, phone and fax numbers, firm affiliations and titles).
   - **Tracking information that our web server automatically recognizes each time you visit one of our sites or communicate with us by email** (for example, your domain name, your email address, and what pages you visit).
   - **Information you volunteer, via applications or surveys** (for example, education, designations, specialties, affiliations with other real estate organizations, and general demo graphic data).
2. **NAR uses this information to Improve and customize the content and layout of our sites and other communications tools, such as REALTOR® Magazine online and print.**
   - **Notify you of updates to our sites.**
   - **Notify you of relevant products and services. Notify you of upcoming events and programs.**
   - **Compile specialty directories about which you will be made aware**
   - **Track usage of our sites.**
   - **Assist local and state REALTOR® associations and affiliated Institutes, Societies, and Councils in membership tracking and for their use for purposes similar to those listed above.**
3. **Email contact information. NAR does not share, sell, or trade email addresses, except that state and local association staff and leadership email addresses may be listed in the membership directories available on NAR.realtor. NAR may use your email address to directly send you information and may provide you with online informational or marketing messages that have been approved by NAR together with other communications to which you have subscribed.**
4. **Other forms of contact information. Forms of contact information other than email address (for example, street address) may be listed in the membership directories available on NAR.realtor. NAR will not share, sell, or otherwise provide this contact information about you except for the following purposes:**
   - **Partners in our REALTOR Benefits® Program for the limited purpose of notifying you of NAR approved promotions.**
   - **Exhibitors at REALTOR® trade shows for the limited purpose of contacting you one time immediately before and after trade shows, through marketing vehicles approved by NAR. Other vendors for the limited purpose of contacting targeted groups of members, through marketing vehicles approved by NAR.**
   - **When required by law or valid legal process, or to protect the personal safety of our members or the public.**
   - **Some or all of the data collected during promotions or contests on our sites that are sponsored by third parties may be shared with the sponsor for the limited purpose of a time marketing follow up by the sponsor. If information about you will be shared with a sponsor, you will be notified prior to your participation in the promotion or contest, and you can decide not to participate in the promotion or contest.**

5. Credit information that you and credit authorizers provide when you make payments by credit card or electronic check for products, dues, or other services via the REALTOR® Electronic Commerce Network will only be used to process the transactions you request. This information will be provided to and maintained by reputable credit reporting databases but will never be sold, shared, or provided to other third parties.
6. NAR follows generally accepted standards to protect the nformation it collects and makes available via its websites. NAR tests their security procedures regularly and modifies them as new technologies become feasible.
7. NAR utilizes a strict Opt Out policy for sending online notifi cations regarding services, products, and programs. You may adjust your Communication Preferences by reviewing your NAR.realtor registration. Just log in first. Then you can change your preferences.
8. You may edit your personal contact information directly in the NRDS system or by contacting your local REALTOR® association.
9. Some of our websites contain advertising placed by advertising networks pursuant to agreements between NAR and the advertising network. NAR does not control these advertising networks, the sites of third parties reached through links on our site, or their information collection practices, and NAR will not be responsible for the activities of these third parties. The advertising network uses cookies to collect certain personally identifiable information when you click on the banner ads appearing on our sites. This information is collected by the advertising network for purposes of measuring and reporting on the advertising to advertisers and NAR. The advertising network may also aggregate the information for certain other statistical and reporting purposes.
10. **Do Not Track Disclosure:** Some browsers have a "Do Not Track" feature that allows you to communicate to websites that you do not want to have your online activities tracked. Our system does not respond to Do Not Track requests or headers from some or all browsers at this time.

The following privacy policy was created by Realtors Property Resource® ("RPR") and is maintained on narrpr.com. This policy is intended to provide an example for developing a privacy policy tailored to your business's specific circumstances, and this policy does contain language pertaining to RPR's obligations under the CCPA.

REALTORS® PROPERTY RESOURCE PRIVACY POLICY

This privacy policy was created by Realtors Property Resource® ("RPR") and is maintained on narrpr.com. This policy is intended to provide an example for developing a privacy policy tailored to your business' specific circumstances, and this policy does contain language pertaining to RPR's obligations under the CCPA.

Welcome to the Realtors Property Resource®, LLC ("RPR") website ("Site"). We at RPR recognize and respect the privacy expectations of our users. We believe that making you aware of how we collect information about you and about your usage of the Site, how we use that information, and who we share that information with will form the basis for a relationship of trust between RPR and you. This Privacy Policy provides that explanation. By using RPR's Site, you consent to RPR's processing your information as set forth in this Privacy Policy, the Privacy Notice for California Residents (if applicable), and any amendments to either. We reserve the right to change this Privacy Policy from time to time.

COLLECTION OF INFORMATION

When you access and use the Site, it may use technology to automatically collect certain information about you, including your activities over time and across third-party websites, apps or other online services. This is called "behavioral tracking." RPR does not respond to "do not track" signals at this time.

In the course of our business, we may collect information from:

- Your usage of the Site;
- Communications, applications, or other forms we receive from you or your authorized representative;
- Your transactions with, or from the services performed by, us, our affiliates, or others including our parent, the National Association of REALTORS® ("NAR");

- An MLS (or broker) of which you are a participant/subscriber.
- "Cookies" that are used to store and track your preferences in order to provide you with customized and personalized services. A cookie is data sent to your Internet browser from a Web server and stored on your computer hard drive. Cookies make your Web experience easier by storing usage patterns and preferences. Cookies are used by most Internet websites and mobile applications. Cookies are required to use RPR's Site, including third-party cookies that provide RPR with usage tracking services, in order to personalize your use of the Site and to create content derived from your usage behavior.

USAGE AND DISCLOSURE

In general, RPR uses the information collected to provide services and to communicate with you. RPR will only share information in the following circumstances:

- When you consent or direct RPR to share the information;
- When RPR provides information to NAR, affiliated companies, service or content providers pursuant to an agreement or to manage and use on our behalf;
- When necessary to comply with a legal requirement or to protect the rights, property, or personal safety of RPR, its users, or the public against harm;
- To enforce or investigate a potential violation of the Terms of Use;
- To detect, prevent, or otherwise respond to fraud, security; or technical concerns; or
- In the event that RPR or NAR is involved in a merger, acquisition, or any form of sale of some or all of its business, your information may be shared with its successor or assigns.

THIRD PARTY WEBSITES

RPR may include links to the websites of other entities. These third-party websites may collect personal information about visitors and users, and this RPR Privacy Policy does not govern collection and use of any such personal information. By accessing any link to websites of other entities via RPR's Site, you acknowledge and agree that your identification information with RPR may be shared with such third party. Please review the privacy policy of each third party for relevant terms regarding collection and use of any personal information by such third party.

CONTACTING RPR

If you have any questions about this RPR Privacy Policy, or the privacy practices of RPR, please contact us at **support@narrpr.com**.

CONCLUSION

As aforementioned, there is no one-size-fits all approach to data security and compliance. It is therefore important that you work with your personal counsel and other relevant professionals who should further advise you on developing a data security program that is tailored to serve the particular needs and interests of your business.

If you have any questions about this Data Privacy and Security Toolkit, please contact the NAR Legal Affairs team at **LegalAffairs@nar.realtor**.

430 North Michigan Avenue • Chicago, IL 60611-4087
800.874.6500 • nar.realtor