Welcome to Window to the Law. I'm Jessica Edgerton, Associate Counsel with the National Association of REALTORS®.

Today we are taking a brief look at how implementing a robust data security program can protect your clients and your business from cybercrime, and keep you in compliance with the law.

Please note that while the information I present in this video applies across the board, state laws concerning data security do vary widely, so be sure to consult with your local counsel during the development of any data security program.

The Federal Trade Commission has published a list of five key principles for businesses to follow when creating a data security program. Those principles are:

1. Take Stock. Have a complete understanding of what data you have in your possession – in your files, your computers, email accounts, cloud storage, and any transaction management platforms your business may use.

2. Scale Down. Keep only the information you need for your business – and this includes any information you need to retain in order to comply with the law. Having a Data Retention and Destruction Policy – which I will discuss in a moment – will be of great benefit in complying with this principle.

3. Lock It. Implement appropriate technology and physical safety measures in order to prevent unauthorized access to your data.

4. Pitch It. Properly dispose of data you no longer need. Again, a Data Retention and Destruction Policy is going to be essential here.

And finally,

5. Plan Ahead. Include a plan for what to do in the case of a data security breach. Be aware that many states require businesses to notify potentially affected parties when a breach has occurred. So – again –being familiar with your state's laws is key during the program creation process.

I've referenced a "Data Retention and Destruction Policy" a couple of times already. This is because every good data security program will include this kind of policy. What does it do? A Data Retention and Destruction Policy sets forth the proper storage and disposal of all data in your business's possession and control. Businesses will want to craft this policy to fit their particular business model. To this end, the National Association of REALTORS® has created a Data Security and Privacy Toolkit, which includes a series of checklists that will help you develop a Document Retention and Destruction Policy to suit your business's particular needs. I will provide a link to that Toolkit in a moment.

As a general matter, however, the essential terms of an effective document retention and destruction policy will address the following:

- First, Identification of the sources and types of information in your business's possession;

NATIONAL
ASSOCIATION *of*
REALTORS®

- Second, how long certain documents are to be retained, and

- Third, the proper storage, and disposal of all data in your possession. This includes specifically addressing the proper handling of sensitive or confidential information. A note here: Many states have laws concerning proper handling of what is known as "Personally identifiable information," or PII. While states' definitions of PII differ, they generally include an individual's first name or first initial, in combination with some other piece of data such as a social security number or address. It is vital that you understand your state's definition of PII, and incorporate it into your policy.

Finally, always remember that the best data security program in the world is worthless if the people charged with implementing it are asleep at the wheel. Keeping your team members educated and engaged in data security is your most important line of defense against cybercrime.

NAR's Data Security and Privacy Toolkit provides a comprehensive overview of data security program implementation, and sets forth the various state and federal laws addressing data security. Please visit this address to access and download the Toolkit.

And thank you for watching Window to the Law.