



Protect Your Business and Your Applicants: 5 Tips for Leasing Office Data Security

By Mike Lapsley, General Manager and Vice President, RentGrow, Inc.



With identity theft and data breaches becoming more commonplace in today's high-tech world, information security is an increasingly important responsibility for businesses.

As a large data provider to the multifamily industry, RentGrow is in-tune with regulations surrounding data security and would like to offer some helpful tips to ensure that your business is doing what it can to maintain a secure environment, and comply with the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions (FACT) Act.

The FACT Act of 2003 provides guidelines for storage and disposal of consumer information such as credit reports. It is important that property management companies, in conjunction with their legal counsel, determine data security best practices that are in compliance with the FACT Act.

5 TIPS FOR LEASING OFFICE DATA SECURITY

Review the following tips to learn about best practices for data security and to ensure that you have systems in place to protect your applicants' privacy.

1. Maximize Desktop Security

Limit electronic access to private applicant information to only those employees who need information to fulfill their job requirements. It is recommended to protect computer access for each authorized employee with a unique password of appropriate strength and complexity (not "123456" or "password1"). Intelligent passwords are crucial because simple and easy to guess passwords are still a common way for hackers to access sensitive information. Update passwords every 90 days and set automatic logouts so that the computer will lock after a set time of inactivity. Be sure to document all employees with access and what systems they have access to.

2. Raise Awareness of Laptop Security

Laptop security is a critical part of data security due diligence. Human error, such as lost or stolen laptops, is the largest single cause of data security breaches and accounts for over 35% of reported incidents, according to the Identity Theft Resource Center of San Diego. Aside from following electronic security protocol, it is wise to educate your

staff about the risks of theft outside your secure office environment. Make your employees aware of responsible laptop transport and handling protocol to minimize risk.

3. Protocol for Staff Changes

In the event of a staff change, it is imperative for companies to have procedures in place to immediately terminate access to applicant data for former employees. In a massive security breach at a large data company in 2005, one way thieves stole personal information was by using log-in names assigned to former employees. To protect against theft, assign an individual to be responsible for terminating access. Upon review of documented checklists of all access granted to former employees, the responsible individual must immediately deactivate and terminate all access privileges, in all systems.

4. Securely Store Hard Copies

Although data storage is clearly trending toward paperless, many companies still store applicant information as a hard copy. If so, be sure to store these paper files securely. Lock all file cabinets and offices storing private applicant data to protect against internal or external theft. Document and restrict access to these storage spaces to employees with permissible purpose.

5. Properly Dispose of Unnecessary Electronic Files and Documents

Businesses must strike a balance between legal requirements for storing data and data security due diligence regarding disposal of sensitive applicant information.

Once storage requirements are met, it is best to immediately destroy all unneeded documents containing personal information to a point where the information cannot be reconstructed or reused in any way.

Conclusion

Today, it's more important than ever to make sure your business complies with the FACT Act to successfully defend against litigation from applicants, a damaged reputation, and associated financial penalties. Be sure your company is complying with data security regulations and conducting due diligence for the good of your clients, your business and the public.

This article is meant to provide education and information on this topic, and should not be construed as official legal advice. All property management companies should consult with their legal counsel regarding their organization's data security policies.

Mike Lapsley is General Manager and Vice President of RentGrow, Inc., the resident screening experts (www.rentgrow.com). He can be reached at lapsley@rentgrow.com.