BY JAREN LYKINS

Get Off of My Cloud

Before moving data to the cloud, it's important to follow proper security measures to protect sensitive information.

After considering the advantages of cloud computing—from its mobile accessibility to cost-savings—many construction companies have decided to move to the cloud. While accessibility has been one of the biggest advantages to cloud-based systems, it can also result in a data security breach.

As technology has become mobile and wireless, it has also made us more vulnerable. Anyone can potentially access your company's sensitive data from anywhere if you do not follow proper security measures.

SHOP FOR SECURITY

When shopping for a cloud software solution provider, be sure they offer a secure Web browser interface. Secure websites have become commonplace—from logging into your bank account to checking your Web-based email.

A secure website will have an SSL Certi cate (Secure Sockets Layer), which will be represented in the Web browser address as https://, and it will have a lock icon. SSL encrypts any information passed between your device (tablet, laptop or smartphone) to your cloud host server.

If you do not use a secure cloud website interface, any sensitive information, such as passwords, social security numbers and credit card numbers, may be readable to anyone attempting to breach the system. SSL also ensures users connect to the right server and not a hijacked server posing as your cloud server.

CREATE AN INTERNAL SECURITY POLICY

Once you have found a cloud-based provider, you should then create an extensive internal company security policy. Certain employees will have access to sensitive company information, such as payroll and company nancials. Policies should be in place explaining how to administer and manage passwords.

Personally created passwords can be easy to remember, but they are often weak and easy to crack. Do not use common words, names or strings of numbers. Use a combination of upper and lowercase letters, numbers

You must understand who your actual cloud hosting provider is, where your data lives and what services they provide to maintain data integrity and protection.

and special characters. Many websites, such as www.passwordtester.com and www.passwordmeter.com, offer an online password strength checker to test passwords and provide tips in creating secure passwords.

Once strong passwords have been established, they should be changed periodically. You should also have a policy in place that addresses how to properly and immediately handle accounts and passwords for terminated employees.

While establishing a company security policy, a user security level analysis should also take place. Many software solution providers offer multilevel security, which allows the administrator to specify applications and functions employees can use.

Create unique, individual logins, and avoid establishing common or shared logins to easily trace any security issues to individual users. Enforcing password and user policies may be time-consuming, but a comprehensive user security infrastructure will allow companies to better manage and protect their cloud data.

ENSURE DATA INTEGRITY

In a traditional of ce network where construction management software runs on the company's work stations and servers, the data resides in that of ce, giving the company control of the data. However, on a cloud-based server, the data lives outside of the company's control. The servers can even reside thousands of miles away.

Some construction management software programs use the software provider's own cloud hosting servers, while other software providers contract with a cloud hosting service.

You must understand who your actual cloud hosting provider is, where your data lives and what services they provide to maintain data integrity and protection. The company and its data center should be certi ed and secure and be a PCI certi ed member (PCI Certi cation sets security standards for data protection).

Also, be sure the cloud host has passed an industry standard audit for information technology, such as the SSAE 16 or SAS 70. Cloud hosts that have passed this audit will have protocols in place if your servers go down or crash. They will also have multi-server mirrored backups of your entire system to get your software and data back up quickly, if not instantaneously.

Even though your cloud host will automatically back up your data by creating system mirrors, it will be your responsibility to ensure the cloud software provider also has policies in place to back up your company's data.

Look for business management software that has a backup utility built into its application that will give you the ability to create timely backups and download the data to your own system or network. To ensure that any failure will be short-lived and very minimal data will be lost, you need multiple levels of backup for multiple sites.

Try This

- Create policies explaining how to administrate and manage passwords for cloud software.
- Once strong passwords have been established, change them periodically.
- Also, establish a policy that addresses how to properly and immediately handle accounts and passwords for users who have been terminated.

After you conduct solid research and investigate cloud-based solutions, you will find a secure and trusted software product that fits your company's needs. However, having the most secure product on the market is only part of the solution.

Construction companies must ensure they install proper security policies, from strong passwords and redundant backups to internal security accountability. Construction companies that work with their cloud solution provider will have a safe and secure environment for data. CBO

Jaren Lykins is an IT Specialist with Deneb Inc., a cloud product software solutions developer for the construction industry. Lykins is responsible for corporate systems administration. For more information, visit www.denebsoftware.com.