Cloudsfer
Powered By Tzunami

Ebook

Master Autodesk Construction Cloud Projects Security in 5 Simple Steps

Step 1: Understand the problems and misconceptions

1 Misconception 1: My cloud provider is solely responsible for data security

Cloud providers are not entirely responsible for your data security, as is commonly believed. Although cloud providers do implement strong security measures, they clearly state in their terms and conditions that the organization is the one who is responsible for protecting the data and that it is its responsibility to take active steps.

2 Misconception 2: My Cloud Infrastructure is Completely Secure

Misconception 2: My Cloud Infrastructure is Completely Secure
Some people think that top construction cloud solutions such as Autodesk construction cloud and BIM 360 are completely secure. While these platforms offer excellent security features, they are not foolproof. Your data can still be vulnerable to insider threats, accidental deletions, and cyber attacks.

3 Misconception 3: My cloud provider provides all the backup I need

Although top construction cloud providers do offer features like Recycle Bins and Vaults to store accidentally deleted files, you must be aware that these options have limitations. They are prone to offer limited time accessibility to deleted files and don't provide a comprehensive backup and recovery solution.

Step 2: Face the Risks Head-On

Data Loss In Numbers

Data loss is expensive and a business-killer

only **6%**

of companies survive for more than two years after experiencing data loss

Cloud Data Loss Factors

1. Cyber attacks

USD 4.45 M

The global average cost of a data breach in 2023

2.Human error

75%

Of data loss causes is from human error

3.Cloud providers short retention policy

only **30** days

The average time most cloud providers offer for storing files in recycle bin policies before permanent deletion.

Step 3: Discover What the Experts Recommend

Microsoft

"We recommend that you regularly back up your content and data that you store on the services or store using third-party apps and services."

Google

"You have a limited time from when the data is permanently deleted to restore files and messages; after that, the data is gone forever."

Dropbox

"Deleted files are marked for deletion in our system and are purged from our storage servers. They can no longer be recovered.

AUTODESK Construction Cloud

"Customers are responsible for ensuring they secure backup copies of their content at all times"

aws

"The customer is responsible for taking active security measures as part of their obligations"

Gartner

"Assuming SAAS applications don't require backup is dangerous"

Step 4: Learn the Essentials of Cloud Security

What does ‘Shared Responsibilty Model’ mean?

The **shared responsibility model** is a framework that delineates the security responsibilities between the cloud service provider and the customer in a cloud-computing environment. In this model**, the cloud provider is typically responsible for securing the underlying infrastructure**, which includes data centers, networking equipment, and tasks like patching and updating operating systems. They also ensure the availability and reliability of cloud services. **Cloud customers are responsible for securing their own data** and applications.

Security best practices: Multi-Factor Authentication (MFA) and Single Sign-On (SSO)

Multi-Factor Authentication (MFA): This is an extra layer of security that asks users to verify their identity in more than one way before accessing an account.

Single Sign-On (SSO): SSO allows users to log in once and access multiple applications or systems without needing to log in again. Think of it as a "master key" – with one login, you can access all your authorized apps.

These methods help to ensure that only authorized users can access sensitive information.

What does ‘Business countinutiy plan’ mean?

BCP is your plan to make sure the business can keep running even if something goes wrong, like a natural disaster, cyberattack, or power outage.

The plan should include:

- Risk Assessment
- Roles and Responsibilities Arrangement
- Backup and Recovery Plan
- Testing and Training Plan

Do you have a BCP in place?

Get to know your ‘Recovery Time Objective (RTO)’ and ‘Recovery Point Objective (RPO)’

RTO refers to the maximum amount of time it should take to restore services after a disruption.

RPO refers to the maximum amount of data loss acceptable between the last backup and the point of failure

Can you tell what are your **RTO** and **RPO**?

More resources *to educate yourself on Autodesk Construction Cloud security:*

- *Autodesk Security Whitepaper – Detailed insights into Autodesk’s security practices for Construction Cloud.*
- *Cloudsfer Blog – Explore security-related topics on the Cloudsfer blog for practical tips.*

Step 5: Start to Act - Turn Knowledge into Action

ACC Secure Cloud Checklist:

□ Set up automation for **backups with Cloudsfer**.

□ Implement **regular security audits**.

□ Provide **ongoing team training** to keep everyone informed on the latest security practices (found on the Autodesk website).

□ Use **monitoring tools** to detect threats early and establish a quick-response plan for incidents.

By relying solely on their cloud providers for data security, many companies unknowingly compromise their operations.
From data loss to costly downtime, misunderstandings about who is responsible for data protection can have severe consequences.

About Cloudsfer backup solution for Autodesk Construction Cloud

AUTODESK Construction Cloud Gold Partner

Cloudsfer is a cloud-to-coud migration and backup platform, provides automated and secure backup solutions specifically for ACC, recognized as **Autodesk Construction Cloud Gold Partner**.

Cloudsfer enables:

Automated Backups
Regularly back up ACC projects without manual intervention, A "set & forget" option is suggested

Storage That You Choose
Integrate with your preferred backup storage like Azure Blob, Amazon S3 / compatible or file system.

Restore At a Press Of a Button
Disaster in place? Quickly recover entire projects or specific files with a few clicks.

Detect Threats in Your Data
Stay informed with detailed backup reports and proactive system threat detection.

Expert Support Always Available
Get round-the-clock assistance for troubleshooting and custom configuration.

Avoid becoming the next data loss victim >>>

Book a demo

Cloudsfer
Powered By Tzunami