Cloud Storage Retention and Integrity Policy

Contents

Cloud Storage Retention and Integrity Policy

1. Purpose

To ensure Kimley-Horn defines guidelines for retention, backup, and archiving of data stored in cloud services. Kimley-Horn's goal is to ensure data integrity, accessibility, and security while utilizing cloud storage providers for collaboration.

2. Scope

This policy applies to all employees, contractors, clients, and third-party service providers who have access to data stored in the cloud managed by Kimley-Horn or its providers.

3. Definitions

Backups
Short-term copies of active data created for the purpose of quick restoration in case of data loss, corruption, or disaster.

Reference Data
Inactive Project data static in nature intended to be informative and supportive.

Archives
Secure long-term storage of data files and datasets, ensuring their immutability. Once data is archived, it cannot be altered, maintaining its original integrity and authenticity for future needs.

Data Integrity
The accuracy, completeness, and reliability of data throughout its lifecycle.

Data Versioning
Best practice for assigning unique identifiers to different versions of data files or datasets to track changes over time. Users are expected to save, retrieve, and revert to these specific versions as needed.

SLA (Service Level Agreement)
A contractual agreement between Kimley-Horn and the cloud storage vendor that defines the expected level of service, including data integrity, availability and access.

4. Policy Details

4.1 Data Backups

Backups will be performed for all critical data.

Cloud Storage Retention and Integrity Policy

- *Defined by vendor, service, business, and IT Requirement. See Appendix for vendor specific requirements.*
- *Backup frequency will be determined based on the data's criticality and the operational requirements within limitations of the selected provider.*

Backup retention period will be XX days, after which old backups will be automatically deleted.
Backup data will be encrypted in transit and at rest.

4.2 Data Archives

Data identified for archiving will be transferred to a long-term storage solution.

- Archived data will have a retention period based on legal and business requirements, with a minimum retention period of 12 years plus 1 day pursuant to Kimley-Horn's records management policy.
- Access to archived data will be restricted to authorized personnel.
- Archived data is immutable and to be unchanged (read only).
- Archived data will be reviewed annually to determine if business requirement of 12 years and a day is necessary.
- Archive data will be encrypted in transit and at rest.
- Kimley-Horn will continue to implement the 3-2-1 Rule for Data Archive and Integrity.
    - We will maintain 3 copies of our data.
    - 2 copies on different mediums.
    - At least 1 copy held offsite.

4.3 Data Integrity SLA

Kimley-Horn will maintain a Data Integrity SLA with the cloud storage vendor that specifies:

- Regular data integrity checks and validation procedures.
- Immediate notification and remediation processes for any data integrity issues.
- Data availability and access commitments, including uptime and recovery objectives.

4.4 Data Access and Security

Access to both backups and archives will be controlled through role-based access controls (RBAC), ensuring that only authorized personnel can retrieve or modify data.

Data will be encrypted in transit and at rest to protect against unauthorized access and ensure confidentiality.

5. Responsibilities

IT Department: Implement and manage the backup and archiving processes, ensure compliance with the Data Integrity SLA, and manage access controls.

Cloud Storage Retention and Integrity Policy

- Implement and manage will be in the constraints of the service provider. See Appendix for specific details around each provider.

Legal and Compliance: Define data retention requirements based on legal and regulatory obligations.

Cloud Storage Vendor: Meet the commitments outlined in the SLA, including data integrity, availability, and security measures.

6. Review and Revision

This policy will be reviewed annually or as required by changes in legal, regulatory, or business needs. Revisions will be made to ensure ongoing compliance and effectiveness of the data management strategy.

7. Vendor Specific Strategy

7.01 Nasuni

Archive –

Backup – 1 Year

Versioning -

7.02 Autodesk Cloud

7.03 Bluebeam

7.04 Bentley ProjectWise

Archive –

- **Archived Data**: Data identified for archiving will be transferred to a designated long-term storage solution.
- **Retention Period**: The retention period for archived data will be based on legal and business requirements. Specifically, we will adhere to a minimum retention period of **12 years plus 1 day**, as outlined in Kimley-Horn's records management policy.

Backup –

1. **Vendor Managed Backup**:
    - Bentley is our partner to manage data backups.
    - Bentley will handle the technical aspects of backing up our data.
2. **Restoration Process and SLA**:
    - The restoration process (i.e., recovering data from backups) is governed by Bentley's **Service Level Agreement (SLA)**.
    - This means that Bentley commits to specific response times and procedures for data restoration.
3. **Backup Frequency**:

Cloud Storage Retention and Integrity Policy

- Bentley will determine how often backups of their system are performed. *(CAPTURE WHAT THIS IS)*
- The frequency aligns with their best practices.

4. **Data Retention**:
   - Our data will remain in place within ProjectWise until it is no longer actively used for collaboration.
   - Once it transitions out of the collaborative phase, it will be ready for archival.

Versioning -

7.05 Citrix ShareFile

7.06 Microsoft SharePoint

7.07 Microsoft OneDrive

7.08 Microsoft Azure

7.09 Amazon Web Services

7.1 Preveil

7.2 ESRI ArcGIS Server

Cloud Storage Retention and Integrity Policy