Data Archiving Policy

Introduction

Data archiving is the process of identifying inactive data and moving it to a secure, long-term storage location, separate from active production data. In this manner, data can be readily retrieved when required without affecting system functionality, clogging up available storage, or jeopardizing adherence to regulations.
A formal document known as a data archiving policy describes an organization's long-term data storage strategy, including what data should be archived, for how long, how it should be secured, and who is in charge of the procedure. Setting up protocols for data retrieval or disposal, designating roles for data governance, defining retention periods for various data types, and putting security measures like encryption and access controls in place to guarantee compliance and stop illegal access are all essential elements.

Archiving criteria

Clear standards for transferring data to archival storage should be outlined in a strong archiving policy. Although age plays a significant role, other factors are just as crucial:

- Age of Data: Data that is older than a certain amount of time, usually 12 to 24 months, is considered for archiving.
- Access Frequency: Data that hasn't been accessed in the last 3–6 months can be archived.
- Business Relevance: Data that is no longer needed for operations, reporting, or analytics can be archived.
- Legal and Compliance Requirements: Data that is subject to retention rules or legal holds must be stored according to those rules.
- Data Sensitivity: To keep people from getting sensitive information, it must be encrypted and stored safely.

Archiving Process

There are several steps in the archiving process to make sure that data is safe, secure, and can be found again in the future:

1. Identifying and classifying data
    - Find datasets that aren't being used or are only being used a little bit.

- Sort data by type, how sensitive it is, and how long it needs to be kept.

2. Getting Ready to Archive
    - To make sure the data is correct, clean it and check it.
    - Add metadata, such as the date of creation, the date of last access, and ownership information.

3. Moving Data to Archival Storage
    - Put data in safe and cheap archival storage, like cloud cold storage or systems that are not connected to the internet.
    - Make sure that data is encrypted both when it is being sent and when it is not being used.

4. Retrieval and Indexing
    - To enable quick search and retrieval, keep your metadata and indexes up to date.
    - Put in place role-based access controls and keep tabs on all retrieval operations.

5. Keeping and Eliminating
    - Keep archived data for a predetermined amount of time, usually three to seven years, or as long as the law requires.
    - When the retention period is up, securely destroy the data using techniques like shredding or overwriting.

Benefits of a Data Archiving Policy

Implementing a structured archiving policy provides several advantages:

- By lowering the amount of active data that needs to be transferred, archiving helps make system migrations and upgrades go more smoothly by minimizing downtime and possible data loss.
- Archiving helps maintain cleaner, more relevant datasets in production systems by separating historical data from current operational data, thereby enhancing the accuracy and quality of data.
- Organizations can increase backup frequency and lower the risk of data loss by drastically cutting down on backup times when there is less active data to process.
- Uses encryption and restricted access to safeguard private information.

References

Proofpoint. (2025, May 19). What Is Data Archiving? Definition & Benefits. Proofpoint. https://www.proofpoint.com/us/threat-reference/data-archiving

IBM. (2021, November 11). Data lifecycle management (DLM). IBM. https://www.ibm.com/think/topics/data-lifecycle-management

Jatheon. (n.d.). Data Archiving Benefits. Jatheon. https://jatheon.com/blog/data-archiving-benefits/