ManageEngine
DataSecurity Plus

# Data retention best practices

Data retention is the practice of storing data for a specific period based on legal, regulatory, or business requirements. It involves deciding how long different types of data should be kept and when it should be securely deleted. Data retention is important because it ensures compliance with laws like the GDPR and HIPAA, supports legal and audit needs, and helps manage storage efficiently. A well-defined retention policy helps mitigate security risks by limiting the exposure of sensitive or outdated data. Overall, it plays a key role in maintaining data governance, cost control, and organizational accountability.

## 6 recommended practices for effective data retention

### 1. Define clear retention policies

Establish a formal data retention policy that outlines how long each data type must be stored. Include retention timelines based on data classification (e.g., financial, personal). Align these policies with industry regulations like the GDPR, HIPAA, or local data protection laws. Communicate and enforce the policy across departments to ensure uniformity.

### 2. Classify and label data

Categorize data based on its sensitivity, value, and legal requirements. Label data appropriately to determine what should be retained, archived, or deleted. This helps automate retention decisions and support secure handling. Proper classification reduces both risk and storage overhead.

### 3. Automate retention and deletion

Use robust tools to enforce retention schedules automatically. Set triggers for data archiving or deletion once the retention period ends. Automation ensures consistency, reduces manual errors, and supports regulatory compliance. Always verify that deletion methods meet secure disposal standards.

### 4. Scrutinize storage and access control

Ensure that the retained data is encrypted and stored in secure environments. Implement access controls so that only authorized personnel can view or modify retained data. Maintain logs to track accesses and changes for audit purposes. Even archived data must remain protected from unauthorized access or breaches.

### 5. Regularly review and audit retention practices

Schedule periodic audits to ensure data retention policies are followed accurately. Identify gaps, unnecessary data stored, or policy deviations during audits. Update retention timelines as per local laws or business requirements. Periodic review helps avoid legal risks and improves data hygiene.

### 6. Educate employees and stakeholders

Train employees on data retention requirements relevant to their roles. Make sure employees know how to store, label, delete, and dispose of data correctly. Promote awareness of legal and cybersecurity risks related to improper data retention.

## Next steps

- Free trial

  Set up and evaluate DataSecurity Plus's capabilities with a free, fully functional 30-day trial.

- Interactive demo

  View an online instance of DataSecurity Plus (available without signing up).

- Guided product tour

  Schedule a demo to have a product expert walk you through the software and answer your questions.

- Request a quote

  View pricing details and request a personalized quote

## About DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It also analyzes file storage and security permissions, deletes junk files, and detects file security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing PII, PCI, and ePHI. It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage.

$ Get Quote

⤓ Download free trial