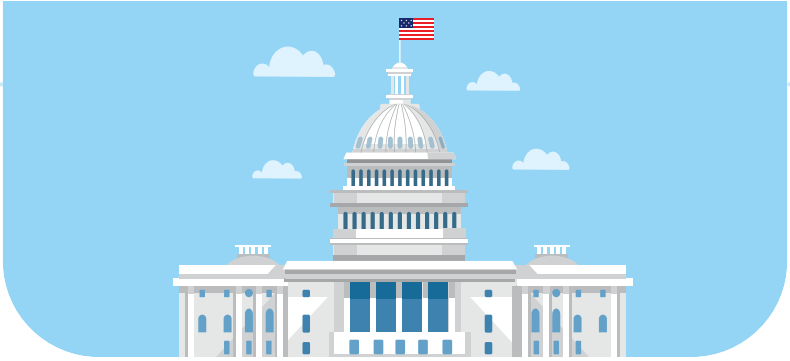
ARTICLE

Dropsuite



Scalable, Secure Cloud Data Backup & Recovery for the Government and Public Sector Ecosystem

Effective data governance, including comprehensive cloud backup and recovery, is more important than ever for government agencies and the many organizations they interact with due to escalating cyber threats, increasing digital transformation initiatives, the need to comply with data protection regulations, and the expanding volume of data that must be managed. The United States government continues to create regulations related to data management, including data security and retention. Compliance with these regulations can be challenging, particularly those that include the public sector and organizations that work with them.

In this article, we will decipher:

- The government standards related to cloud backup and recovery
- The need for a simple solution for agencies and third parties to back up and restore sensitive and classified data securely
- The technical capabilities you should look for
- Common use cases that illustrate the many data-related regulations that apply to government agencies and those that work with them
- How you can meet these requirements for scalable, secure cloud backup and recovery

Government Standards in Cloud Backup & Recovery

As organizations of all types have moved to the cloud, the federal government has sought to keep up with technological developments.

In 2011, the Office of Management and Budget (OMB) released the Cloud First strategy as part of its Federal Government IT Modernization efforts, requiring the federal government to move to the cloud without providing guidance on how to accomplish that goal. At the same time, the Federal Risk and Authorization Management Program (FedRAMP) began to ensure the security of cloud services used by the government.

In 2018, the OMB updated from Cloud First to the Cloud Smart strategy, which offered more practical implementation guidance and was founded on three pillars: security, procurement, and workforce.

This shift, spurred by rapid digitalization, increased the volume of digital data generated by the government, all of which needed to be easy to manage, store, and retrieve. Cloud backup and archiving offer a cost-effective, scalable alternative to on-premises servers and data centers for the public sector ecosystem, just as it does for the private sector.

Cloud solutions are appealing because they can ensure that essential data is not lost in the case of a successful cyberattack or other types of disaster, such as:

- Equipment failures
- Localized power outages
- Civil emergencies
- Natural disasters
- Criminal or military attacks

Keeping that data safe and secure also helps organizations meet regulatory requirements, such as the Federal Records Act and the directive from the National Archives and Records Administration (NARA) to all federal agencies to manage emails electronically by the end of 2016 and all additional records by 2022.

As cyber threats have increased and become more complex,

using FedRAMP-compliant cloud products and services has become a critical way to help the public sector ensure cloud service security. And because more data privacy regulations and security frameworks are emerging, meeting all those requirements can seem challenging. Organizations face not only mounting cyber threats, but also potential regulatory fines for non-compliance and difficulty in securing cyber insurance. Those challenges are compounded by the complexity of the government ecosystem, which is made up of different players that must work together to ensure that all these requirements are being met, including:

- Managed service providers (MSPs)
- Cloud service providers (CSPs)
- Systems integrators (SIs)
- Independent software vendors (ISVs)
- Government agencies and regulatory bodies

Many organizations rely on MSPs to make it simpler for them to meet the many regulatory needs of their public sector customers.

10 Reasons You Might Need GovCloud Backup

1. You have files that require FedRAMP Moderate compliance
2. You are located in the United States and need to ensure data is stored and processed in compliance with local laws and regulations
3. You work with government agencies or municipalities
4. You want to minimize your chance of data loss in case of disaster, including cyberattacks
5. You want a secure cloud backup that is separate from your primary environment
6. You need to ensure every element, including data storage, transmission, and management, is confined to the United States — as well as the people accessing the data
7. You need to comply with regulations to retain data securely and need that data readily available for audits and reviews
8. You need data to be accessible exclusively to a U.S.-based workforce with explicit permission for access to ensure continuing operations in emergency situations by enabling frequently updated backups, providing data redundancy, assuring rapid data recovery, ensuring remote accessibility, and offering cost-effective scalability
9. You need an automated and incremental backup that is simple to manage
10. You need granular administrative roles to ensure control over data sharing and access

Meet Specific Compliance Needs

The list of regulations related to data privacy and security and data retention may surprise you. Here are two examples to highlight the extensive compliance requirements of diverse types of clients.

Police Departments

Suppose you have a police department as a client. In that case, they will need to comply with various data privacy, security, and retention standards, which can be set by departmental policies as well as at the federal, state, and local levels.

- The Criminal Justice Information Services (CJIS) Security Policy was established by the FBI and includes requirements for the creation, viewing, modification, transmission, dissemination, storage, and destruction of criminal justice information, including policies on data encryption, MFA, remote access, and incident response.
- The Privacy Act of 1974 governs the collection, maintenance, use, and dissemination of PII that federal agencies maintain in systems of record, which may impact local law enforcement agencies when they interact with federal systems or receive federal funding.
- HIPAA may apply to law enforcement agencies when dealing with medical records or other protected health information.
- **State and Local Privacy Laws** may impact how police departments handle information, such as requiring the encryption of certain types of data, reporting data breaches, or handling biometric data.
- **Departmental Policies** may also govern data privacy and security, dictating the use of specific technologies or procedures for data protection.
- Body-Worn Camera (BWC) Policies may govern the use and data management of body-worn cameras due to the privacy implications of the video and audio data collected.

Police departments must also comply with data retention regulations stipulating how long certain data types must be retained before they can be securely disposed of, including criminal records, arrest records, incident and investigation reports, body camera footage, administrative records, and 911 call records.

Compliance with these regulations, standards, and policies is critical for maintaining the public's trust, as well as avoiding legal penalties and ensuring the integrity of criminal investigations.

These standards continue to evolve to keep pace with

technological advancements, so it is necessary to have a robust solution in place to ensure secure cloud data backup that is discoverable and can retain data for the period required.

Law Firms

Law firms in the United States manage extremely sensitive information, including proprietary data, client information, case details, and other confidential records.

As an increasing number of law firms have begun relying on cloud-based solutions for data storage and operations, they too must adhere to the specific requirements for cloud data retention, security, and recovery to ensure compliance with U.S. laws.

- The American Bar Association's Model Rules of Professional Conduct outlines a lawyer's responsibility in preserving client properties, including files and data. Attorneys must also make reasonable efforts to prevent the inadvertent or unauthorized access to or use of client information as well as understand how client data is transmitted and stored.
- The Sarbanes-Oxley Act (SOX) may require the retention of certain types of data, which must be held for specific periods.
- The Health Insurance Portability and Accountability Act (HIPAA) requires that if a law firm handles protected health information (PHI), it must comply with HIPAA's privacy and security rules and implement specific administrative, physical, and technical safeguards.
- Gramm-Leach-Bliley Act (GLBA) applies if a law firm is involved in certain activities related to personal financial information; it may need to comply with GLBA's privacy and safeguards rules.
- The Internal Revenue Service (IRS) Guidelines may require records to be kept for a minimum of three years or longer for some documents.
- **State-specific Cybersecurity Laws** may apply; for example, California and New York have enacted their own cybersecurity and data privacy regulations, which may apply to law firms operating in all states with such requirements.

Law firms must regularly review and update their data privacy, retention, and security policies to ensure compliance with current laws and best practices. Additional standards and regulations may also apply, and all technology, including cloud services, must comply with these requirements.

Introducing Dropsuite's GovCloud Backup

GovCloud Backup is a new offering from Dropsuite that allows users to back up and restore sensitive and classified data in the cloud while maintaining heightened security requirements. GovCloud Backup supports Microsoft 365 (M365) Government Community Cloud (GCC) environments at the moderate level, an environment that provides enhanced security measures and compliance offerings to address the unique needs of the public sector. It was designed for organizations that require compliance with FedRAMP Moderate, HIPAA, and IRS Publication 1075. M365 GCC is hosted in Microsoft's government-only cloud environment, separate from the public cloud. Dropsuite's product backs up data in this environment to another location to meet the requirements for the security of cloud backups for the public sector and ensure the availability of the data.

Dropsuite's GovCloud Backup provides scalable, secure backup for M365 through Amazon Web Services (AWS) GovCloud to ensure the data is held in an environment entirely isolated from M365. GovCloud Backup meets the compliance, security, and operational requirements of most public sector agencies and contractors holding or processing data on behalf of the U.S. government. GovCloud Backup:

- Enables easy, automatic backup of sensitive and classified data in the cloud
- Offers simple, secure data restore capabilities
- Provides availability and discoverability
- Supplies a scalable environment to hold all data generated

GovCloud Backup Technical Details

Reliable Architecture

Dropsuite employs 256-bit AES military-grade encryption at rest, TLS 1.2 in transit, and supports multi-factor authentication (MFA) to provide servers that are compliant with government regulations. Backup to AWS GovCloud's secure environment ensures the redundancy and reliability of your data, meeting the requirement for secure backups that are easy to use, automated, and discoverable.

Easy, Accessible Backup and Transparent Pricing

Dropsuite's GovCloud enables backup within minutes of creating an account, providing automated and incremental backup, and offering the ability to download, restore, and migrate data with a single click. It includes unlimited storage and incurs no ingress or egress fees for moving or transferring data. Pricing is per-user, so you only pay for what you need, and it is free to self-service download or

export data. Access to backups is available from any device or location, ensuring that disaster recovery is simple.

Compliance Features

Dropsuite's GovCloud Backup and Archiving adheres to multiple data privacy regulations, including:

- FedRAMP Moderate
- System and Organization Controls (SOC) 1, 2, and 3
- Federal Information Security Modernization Act (FISMA)
- Payment Card Industry (PCI) Data Security Standard (DSS) (commonly known as PCI DSS) level 1
- ISO 9001 / ISO 27001
- International Traffic in Arms Regulations (ITAR)
- HIPAA

Dropsuite's GovCloud includes regular audits and reports, enabling users to apply compliance tags and review audit and activity logs. These tags and logs, used with the search tool, make locating specific data within backups and archives easier, which is critical during audits and maximizes discoverability. Dropsuite's GovCloud also makes it easy to compile reports to demonstrate compliance with different standards to show data backups, user activity, and more.

To ensure that only authorized users access the data, Dropsuite's GovCloud includes:

- Granular, role-based access control features
- Allowed delegated access
- Limited access user
- Group access by department
- Compliance supervisor access
- Compliance reviewer access
- Data Protection Officer role

Additional GovCloud Backup Security Benefits

Many companies doing business with government entities, and the government entities themselves, must fully adhere to compliance regulations.

Dropsuite's GovCloud Backup makes it easy to meet government standards for enhanced security by providing backup and recovery in AWS GovCloud, which offers both US-East and US-West regions that are operated on U.S. soil by employees who are U.S. citizens. Only U.S. entities and root account holders who pass a screening process can access AWS GovCloud, which helps to ensure that all data is appropriately protected and stored, including:

- Controlled Unclassified Information (CUI)
- Personally Identifiable Information (PII)
- Sensitive patient medical records
- Financial data
- Law enforcement data
- Export controlled technical data

To further ensure a secure environment, Dropsuite conducts annual penetration testing and offers single sign-on (SSO) and MFA to minimize the possibility of unauthorized access to the cloud backup environment.

Scalable, Secure Cloud Data Backup & Recovery

Dropsuite's GovCloud provides the simplicity and scalability of cloud backup and recovery for the government ecosystem by maintaining heightened data security requirements. It provides transparency and control over data hosted in a government-only cloud environment separate from the public cloud and the M365 GCC environment to ensure that it meets the requirements of a wide range of regulations.

As data volumes continue to increase rapidly, GovCloud Backup enables the scalability and cost-effectiveness that MSPs need to provide their clients to ensure they have the access they need, when and where they need it, without subjecting them to hidden fees or holding data hostage.

At the same time, cyberattacks from hacker groups, individuals, and nation-state actors highlight the importance of backing all cloud data up in a separate location from where the data lives. This ensures that even if a cyberattack on the primary data were successful, the backups would remain secure and accessible at any time and from anywhere.

For public sector organizations that interact in the complex government ecosystem, it's essential to have a secure, compliant solution to backup and restore data in the cloud.

This is how Dropsuite can help:

- Dropsuite's GovCloud Backup protects your most important M365 GCC data in the cloud by securely backing it up to AWS GovCloud and restoring any file on demand.
- Dropsuite's eDiscovery solution provides discovery and access for business-critical data in an electronic form for litigation or other compliance needs.
- Insights BI Email Analytics provides a robust analytics toolset that turns complex and extensive email data sets into simple, actionable reports, graphs, and charts.

CONTACT US

For more information, please contact us:
www.dropsuite.com | sales@dropsuite.com

© 2023 Dropsuite Limited. All rights reserved.