nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
Office: +1.617.520.4120

USING NCRYPTED CLOUD TO AID FISMA COMPLIANCE

Overview

The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The Act is meant to improve information security within the Federal Government and affiliated entities, like government contractors, by mandating information security controls and periodic audits. National Institute of Standards and Technology (NIST) is chartered with developing standards, guidelines and publications that federal agencies must follow to implement FISMA.

This white paper outlines how nCrypted Cloud is the industry leading solution to may be used to achieve and maintain FISMA compliance when using cloud-based file storage and sharing facilities such as Dropbox.

Specifically, this white paper details:

- How nCrypted Cloud aids FISMA compliance by implementing specific requirements among security control classes and families described in NIST SP-800-53 Rev 3
- Why nCrypted Cloud is superior to all of the other competitive products

Executive Summary

nCrypted Cloud gives Federal agencies and affiliated organizations the ability to confidently maintain FISMA compliance by enforcing encryption and security controls when using cloud-based file storage and sharing technologies while continuing to leverage the cost benefits and collaboration features these solutions offer.

nCrypted Cloud provides the controls and security safeguards to meet data and access-related Management, Operational, and Technical compliance requirements of FISMA.

nCrypted Cloud offers the most comprehensive and effective solution in the marketplace for securing files stored with cloud storage service providers. nCrypted Cloud is the only solution that persistently encrypts data at rest on mobile devices and traditional personal computers and maintains encryption during synchronization so that data remains encrypted in the cloud.

Cloud-based file storage and sharing – Overview

Cloud-based file storage and sharing is an innovative technology that can be used to access, synchronize, and share documents or files anywhere, anytime, with anyone, and from any device. Numerous cloud-based storage providers exist, however, the most prominent and the market leader is Dropbox.

Cloud storage solutions have become unavoidable in the workplace. They're just too darn simple to use, useful for collaboration, and the free-to-low-cost price point makes perfect business sense. With the right controls in place, cloud-based file storage and sharing can be used to track and monitor activity on the cloud, allowing for better visibility and control of the data, as well as the devices and users that have access to them.

FISMA Overview

Federal Information Security Management Act (FISMA) is a comprehensive framework for securing the federal government's information technology. National Institute of Standards and Technology (NIST) developed IT security standards and guidelines. Federal agencies must follow these rules, which require compliance reporting by each agency on 17 specific security controls spanning across Management, Operational, and Technical classes of controls.

Failure to comply with FISMA results in low grades for the agency and makes it highly susceptible to cyber-attacks, potential security breaches, and impending loss or cancellation of funding for the agency or agency's projects by the Office of Management and Budget (OMB).

How nCrypted Cloud Facilitates FISMA Compliance

nCrypted Cloud security safeguards effectively and efficiently addresses data security elements of the various families of controls developed by NIST for FISMA compliance. There are a number of security features in nCrypted Cloud. The most prominent among them that support FISMA requirements are:

Identification and Authentication: nCrypted Cloud users are required to authenticate themselves to their cloud storage

470 Atlantic Avenue
Boston, MA 02210
Office: +1.617.520.4120

provider as well as nCrypted Cloud prior to accessing the data. There is no provision for anonymous access to data secured by nCrypted Cloud.

Media Protection: nCrypted Cloud allows agencies to apply classification to files and folders in cloud storage solutions like Dropbox, Google Drive, etc. The classification tags applied to the documents may be aligned with NIST's Media Protection requirement of data marking, sanitization, storage, and transport. Classifying the data in real-time using automated policies allows organizations to quickly perform inventory of where data resides.

Access Control: Data stored in cloud storage systems and protected by nCrypted Cloud may be controlled for access by the organization's administrator, data owner, or the appropriate designate as the only explicitly authorized individuals. nCrypted Cloud ensures the protection of sensitive data whether it is stored in the cloud, on a mobile device, or on a traditional personal computer, even when it is synchronized to devices owned by the users.

nCrypted Cloud provides fine-grained privacy access controls such as read, print, or edit privileges, termination date triggers, and water marking at both the folder and document level.

Audit & Accountability: Keeping log of auditable events with event time stamps is a critical control requirement (AU-2, AU-8) published by NIST. nCrypted Cloud provides an indispensable audit trail, documenting who accesses data, what exactly they did, when they did it, and where they did it. This audit trail provides comprehensive event data to account for all access activity providing much needed audit record retention for FISMA compliance.

Additional Security Features

Other strong and attractive security features offered by nCrypted Cloud when using cloud-based storage and sharing technologies are:

Secure Collaboration: nCrypted Cloud users now have the ability to use the same easy interface of cloud storage solution like Dropbox to securely store and share files in the cloud.

Persistent Strong Encryption: Files protected by nCrypted Cloud are always AES-256 bit encrypted, whether they are at rest on the user's computer, synced to any mobile devices, or when they are stored in the cloud.

User and Device Revocation: nCrypted Cloud administrators can at any time revoke user's access to the organization's data resulting in the user instantly losing the ability to view the data, even when the data is already synchronized to the user's personal device. Additionally, devices can be unlinked from the organization to protect against potential data loss caused by a lost/stolen device.

How nCrypted Cloud is Superior

While many competitive products make similar claims, nCrypted Cloud is the only one that offers a complete and comprehensive enterprise solution. nCrypted Cloud's patented technology includes the following features:

- Persistent encryption at all times and in all places
- Feature rich access controls at the document or file level
- Data access inventory
- Extensive event logging and auditing capabilities
- Highly available service hosted in SSAE Type II geographically dispersed data centers

Conclusion

nCrypted Cloud delivers a ground breaking cloud file storage and collaboration security solution that meets, and in many instances exceeds, ITAR requirements. nCrypted Cloud's consumer-centric design, data-centric security architecture, enterprise strength encryption, and auditing features make it the undisputed leader in the marketplace.