Acronis® provides secure and easy-to-use, affordable cloud storage for off-site backups of your files and system image. We are committed to ensuring security and privacy of your data and the following whitepaper is provided to help you better understand and evaluate the security of our online backup service.

Military-grade security of access and privacy of your data

Any data that you backup up to Acronis cloud storage is protected from unauthorized access using industry highest standards of security. We provide you a choice of military-grade encryption options with up to 256 bit key length (many providers use less secure 128-bit encryption only). All backup data is encrypted before uploading to the Internet. Each user of Acronis online backup service is identified by his username (e-mail address) and a password during authentication which is performed securely over SSL. Acronis does not store copies of your encryption keys and cannot at any circumstances access your data.

Better than RAID reliability of cloud storage

Many online backup vendors use traditional RAID architectures that are known to lose reliability properties on particularly large amounts of data. In order to overcome RAID limitations Acronis has been developing since 2008 a proprietary purpose-build cloud infrastructure designed to securely and reliably store your backups. Our specialized storage software running in our datacenters ensures that backups cannot be corrupted or lost even in case of the underlying hardware failure. This is achieved using so called software erasure coding – an advanced method of data integrity verification that overcomes reliability limitations of hardware storage.

Our proprietary software redundancy implementation based on modified Reed-Solomon error correction codes provides an industry leading high level of guaranteed data reliability. The software continuously checks integrity of the backups and is able to recover from even a major hardware failure without the need to resend any affected portions of data from the client to the datacenter. This means that at no time there can be a corrupted or damaged backup on storage, and you are never at risk of being unable to recover the data that was affected by not yet retransmitted from your original system.

Our software automatically identifies problematic hard drives before they fail and proactively copies your data to healthy drives, ensuring that your data is never at risk of hardware failure. This approach effectively eliminates problems like silent data corruption or data loss due to simultaneous multiple hard drive failures that are inherent to traditional hardware RAIDs used in many legacy online backup systems.

High availability of Acronis cloud storage is maintained using distributed clustered architecture with no single point of failure component that could prevent you from accessing your backups in case of a disaster. All components of our software architecture are replicated for redundancy and scalability ensuring that there is never a bottleneck in accessing to our datacenters regardless of how many end-users would be downloading backups, for example, in an event of a geography-wide disaster.

Hardened datacenter facilities

Acronis provides online backup services out of multiple datacenter locations chosen to ensure maximum available internet connectivity and with the consideration for compliance with national data protection regulations. Additionally, in the United States our datacenter provider has been audited in accordance with the requirements of SSAE 16 (formerly SAS Type II).
OVERVIEW

Redundant Power and Networks
Our datacenters are equipped with UPS and backup diesel-generators and are designed to ensure constant power availability for up to 48 hours to sustain an undefined power outage. In addition, there are redundant air conditioning systems, network equipment and power supplies. All our equipment is located behind industry-leading firewalls and all network equipment is provided with network redundancy.

Onsite Monitoring and Security
Physical security is ensured via high fences, 24/7 security personnel, and video surveillance with 90-day archiving. Biometric hand-geometry scan and proximity key card are required for access. Only authorized employees can access physical facilities of the datacenter.

Fire Detection and Suppression
VESDA (Very Early Smoke Detection Apparatus) Air Sampling and Dual Zone Pre-Action (Dry Pipe). There is also temperature and humidity monitoring.

Network bandwidth availability
Acronis does not limit network bandwidth for in and out transfers.

Prerequisites for regulatory compliance
Acronis provides security features such as password protection and encryption of backups that can be used to meet security requirements of certain compliance regulations. These features are sufficient or exceeding the required levels for most common regulations. For example, you can configure and manage your own encryption keys in order to achieve HIPAA compliance in combination with other measures for medical organizations. However Acronis does not warrant or represent that our solutions will satisfy any compliance regulations in particular. It is the sole responsibility of an end-user to evaluate whether or not Acronis’s solutions satisfy regulations the user is seeking to comply with and the user must consult their own experts and attorneys to perform this assessment. Any product specifications or details related to the features of Acronis solutions are provided for your information and to allow you to make this assessment on your own.

Summary
Acronis provides the highest industry-available levels of security for online backups stored in our datacenters. Backups are protected with up to 256-bit key length encryption and stored split across multiple servers which makes it impossible to access even the encrypted backup. Our storage software guarantees backup consistency and availability even in case of hard drive failures, never leaving you unprotected. Our datacenters add another layer of physical security which ensures that you and only you can access your backups at any time when you might need them.

Additional information
To read Acronis full privacy policy, click here http://www.acronis.com/company/privacy.html
To learn more about Acronis online backup solutions visit http://www.acronis.com/solutions/cloud.html
To start a free trial of Acronis online backup, click here: http://www.acronis.com/backup-recovery/online/gettrial.html

For additional information please visit http://www.acronis.com

To purchase Acronis products, visit www.acronis.com or search online for an authorized reseller.

Acronis office details can be found at http://www.acronis.com/company/worldwide.html

Copyright © 2002-2013 Acronis International GmbH. All rights reserved. "Acronis" and the Acronis logo are trademarks of Acronis International GmbH. Other mentioned names may be trademarks or registered trademarks of their respective owners and should be regarded as such. Technical changes and differences from the illustrations are reserved; errors are excepted. 2013-06