Acronis Cloud Data Centers:

A Primer on Security, Privacy, and Compliance

December 2016

Acronis

Table of Contents

Introduction

Cost efficiency, ease of implementation, and outstanding Recovery Time Objectives (RTOs) are key reasons to implement cloud data protection solutions. According to an **ESG study**, use of cloud storage to store backups has tripled from 2012 to 2015.

Since 2003, Acronis has offered industry-leading disaster recovery solutions to businesses of all sizes. Today, law firms, banks, financial institutions — and other organizations with extreme data sensitivity, high security requirements, and zero tolerance for data loss and downtime — trust Acronis to protect their business-critical systems and data.

Acronis has unparalleled experience in designing and executing critical data protection solutions. Acronis Cloud data centers leverage sophisticated enterprise-level security, privacy, and compliance mechanisms for organizations of all sizes. Few of the more than 500,000 Acronis business customers can implement the same level of security on their premises, or in their private clouds, using their own resources.

This document describes Acronis' stringent privacy and data security policies and practices regarding the confidentiality and safety of your data. Given the accelerating rate of change in the information technology industry and its ever-evolving capabilities, technical details in this white paper are subject to change. What never changes is Acronis' unwavering dedication to protect your data.

Information Security

Customers trust Acronis with the safety and security of their information because they recognize that Acronis is continually vigilant and committed to providing the best data protection practices and software.

Information security is not just a steady set of strategies for managing processes, tools, and policies. Rather, information security is an ongoing process. Acronis has invested significant resources to provide enterprise-level security to Acronis customers at a fraction of the cost of other on-premise or private cloud information security solutions.

Experienced and trained personnel constantly maintain, enhance, and verify Acronis' infrastructure. Acronis employs the latest up-to-date software, hardware, technologies, and processes to design, build, operate, and support its services to protect customer data from current known threats and constantly enhance its measures and controls.

Acronis continuously works to improve asset tracking, asset profiling, access control, and vulnerability management to provide consistent services and maintain our level of security. Acronis follows the guidelines of top global information governance standards and practices such as ISO/IEC 27001, PCI DSS, and US NIST (see Physical Security). Acronis actively seeks compliance with additional guideline standards to suit current and future customer needs. All of Acronis' information security measures are integrated and coordinated with the Acronis Business Continuity Management Program to minimize any security threat, natural and human-made.

Data Storage Resilience

Acronis Cloud Data Centers store customer data employing its own software-defined storage solution, Acronis Storage with Acronis CloudRAID™ technology. Acronis Storage delivers fast, universal, protected, efficient, and proven storage that unites block, file, and object workloads.

Acronis Storage utilizes a proprietary erasure-coding algorithm to enhance reliability and protection against failures. It includes scalable and efficient self-healing mechanisms, minimizing data risks. In addition, Acronis Storage utilizes a fully redundant architecture to safeguard data integrity for every customer.

Over the years, storage capacity at the Acronis Data Centers grew from hundreds of terabytes to dozens of petabytes. All the while, the unique flexibility and scalability of Acronis Storage ensures this exponential rate of growth does not affect customer critical data in any way.

Physical Security

Security starts at the Acronis Data Centers. Acronis hosts data and cloud products at trusted data centers that are physically distributed around the globe — in the U.S., UK, Switzerland, France, Germany, Russia, Japan, Singapore, and Australia.

Respected, non-Acronis accreditation organizations regularly audit Acronis Data Centers to ensure support of various certifications. These standards include:

- ISO/IEC 27001
- ISO/IEC 9001
- SSAE 16, Types 1 & 2
- PCI DSS

Acronis Data Centers and Acronis technology are physically supported and secured 24x7x365 to protect against potential attacks using:

- Cages
- Access control cards
- Biometric access control systems
- Fire suppression systems
- Surveillance cameras and notification systems, such as intrusion detection sensors, heat sensors, and smoke detectors

Similar measures protect Acronis business offices and headquarters as well.

Acronis employs the highest standards of physical security at Acronis Data Centers, protecting the safety of customer data. The level of protection from intruders exceeds anything that small to medium businesses can hope to implement alone.

Personnel Security

Maintaining data security is impossible without people. Acronis understands that its main security concern is its employees. No system or infrastructure can be 100 percent protected without training employees and the leadership teams on security awareness, data protection, and privacy as well as Acronis' own security standards.

All US-based employee candidates who have access to systems and data are subject to a standard background check as permitted by law. This includes a review of a candidate's education, employment, and criminal history. Careful handling of information is at the core of Acronis' corporate culture. Every Acronis employee is required to sign a Non-Disclosure Agreement (NDA) as well as a company "Code of Conduct" statement. In addition, Acronis continuously trains personnel so they stay current with evolving information protection guidance and requirements.

Acronis follows the principals of segregation of duties and least privilege. This ensures that every user has the least amount of privilege necessary to complete a job so that only staff with the highest-clearances can access its data centers.

Privacy

Privacy of customer data is Acronis' highest priority. Customer data is defined as "all data, including text, sound, video, image files, and software that are provided to Acronis by or on behalf of the customer using its services."

To maintain the privacy of customer data, Acronis personnel do not have or require password access to client operating environments or client data stored on Acronis premises unless explicitly authorized by the customer. Acronis personnel are unable to authenticate beyond the operating system.

All Acronis users have unique IDs protected with a password. Every user ID is created only after email address verification. The passwords are never stored in plain text; they are stored securely using a strong hashing algorithm with unique **"salt"** for each password.

Acronis is not able to restore user passwords. If the user forgets a password, it can only be reset after email verification.

Data Encryption

All user data sent to Acronis Cloud Data Centers can be encrypted in-transit and at rest. Acronis uses FIPS 140-2 Level 1 certified encryption algorithms. Decryption is only possible with the encryption key, based on the password. Thus, only the user with the correct password can decrypt the data. No other party, including Acronis, can decrypt it without the password.

System Maintenance

To provide continuous maintenance service, Acronis uses sustainable monitoring, which involves constant infrastructure checks via vulnerability scanners. Data that is obtained from the scans allows Acronis to implement a continuous maintenance schedule to keep the infrastructure up-to-date.

Acronis monitors all official repositories and bulletins for the latest information. Security and critical updates have the highest priority and are rapidly installed. Every update is fully tested before it is implemented. Acronis employs skilled technology professionals and experts at every level of its infrastructure and actively collaborates with its third-party vendors to resolve issues. All maintenance and system updates are tracked in an IT Service Management System and are subject to strict internal Service Level Agreements (SLAs).

Network Security

Acronis continuously monitors the security of its entire IT infrastructure to protect against advanced cyber-attacks. Acronis controls and monitors its boundary, DMZ networks, VPN and remote connections, and internal flows. Acronis utilizes automated tools in conjunction with organizational controls to guard against human interventions.

The Acronis network is multi-layered and zone-based. Its customers and internal environments are fully segregated.

Acronis provides real-time encryption for all data transferred between customers and data centers, Acronis employees and data centers, and between the data centers themselves. This provides the best protection for network interaction between office-based users and data centers.

To protect against malware, Acronis uses the most modern web application firewall. It includes instant protection against SQL injection, cross-site scripting, unauthorized resource access, remote file inclusion, and other OWASP (Open Web Application Security) threats.

Acronis' enterprise-grade network security is designed to prevent even the most sophisticated attacks, and offers a level of protection that is extremely difficult for small-to-medium businesses (SMBs) to achieve in their on-premise facilities.

Software Practices

Acronis uses the latest versions of software and regularly updates its operating systems, software, frameworks, and libraries. If a vulnerability in our product or a zero-day vulnerability is publicly reported, Acronis springs into action to mitigate risks. Acronis' software practices safeguard the confidentiality, integrity, and availability of all data.

Standard software security practices include:

- Adherence to strict security requirements and policies, with well-known security best practices applied at every stage of the application lifecycle.
- Regular source code review (manually and using static code analyzers) for security weaknesses, vulnerabilities, and code quality to provide direction and guidance for product development.
- Code assessment and dynamic scanning with manual checks of pre-production environments.
- Security review of architectures, design of features, and solutions.
- Security awareness training for all teams per their respective job roles.

Hardware Maintenance Contracts

Acronis follows the approach of need plus one (N+1) for greater redundancy across all hardware layers of its infrastructure. This ensures that if there is a failure in a hardware-layer component, it does not affect Acronis' critical infrastructure or Acronis customers.

Every piece of equipment is under warranty and all elements of the infrastructure are covered under the respective vendor's SLAs.

A dedicated team manages all vendor maintenance contracts, which are subject to annual review and revision. The team follows a standardized maintenance approach designed to improve infrastructure availability and reduce operating and maintenance costs.

Change Management

Change Management is the process that controls the life cycle of all changes. Its goal is to implement changes with minimum disruption to IT services and business goals.

Acronis tracks all changes to its technology environment. Each change process is assigned a process owner. Every change, from the very beginning through production, goes through the following steps:

- Development
- Quality Assurance (QA) verification
- Stakeholders acceptance
- Implementation team readiness
- Notifications
- Implementation
- QA acceptance
- Postmortem

Acronis announces maintenance and any changes that affect a production environment in advance to allow for sufficient preparation. Acronis commits to send notifications for:

- Planned maintenance — seven days prior to maintenance date
- Unplanned emergency maintenance — 24 hours prior to maintenance date

Additional information or notifications include the following:

- Maintenance start (five minutes before actual start)
- Process is passed to QA for acceptance
- Maintenance will take longer than planned
- Maintenance is complete

Acronis plans non-urgent maintenance for after business hours in the region where the change takes place.

Business Continuity and Disaster Recovery Program

Many potential disruptive threats can occur at any time and affect business operations at any location. Acronis considers a wide range of potential threats as part of its risk analysis assessment at all Acronis locations.

Acronis has a Business and Disaster Recovery Program in place that addresses its critical processes and technology at all its data centers. Currently, Acronis is refreshing and formalizing its internal Business Continuity and Disaster Recovery Program, a process that is expected to continue throughout the first two quarters of 2017. This includes the following elements:

- The review and refresh of existing program information
- Creation of new program information in support of Acronis' comprehensive program for emergency response (people), business continuity (process), disaster recovery (technology), and crisis management
- Company-wide business continuity and disaster recovery policy
- Employee training
- Risk assessment refresh for each Acronis location
- Business-impact analysis to identify critical processes and technology
- An annual update and exercise to test business continuity and disaster recovery plans
- An on-going process to maintain a Crisis Management program that includes the creation of Crisis Response and Management teams for triaging business disruptions, IT incidents, and emergencies

Acronis has established partnerships that run numerous, global, collocated data center facilities. These facilities meet rigorous standards and compliance needs regarding setup, power, and cooling to maintain optimum conditions and uptime to safeguard mission critical data. Additionally, Acronis has numerous data center locations and provides different geographic zones for customers to locate their disaster recovery and critical information away from company locations.

Acronis recognizes the importance of having a comprehensive Business Continuity and Disaster Recovery Planning Program to:

- Protect employee safety
- Safeguard the continuation of critical business processes and technology, both internal and customer facing
- Safeguard Acronis' ability to service its customers without interruption

To that end, Acronis requires the commitment of each employee, department, and vendor to: support its business continuity program objectives; review, build, test, and grow its Business Continuity and Disaster Recovery Program; and protect Acronis assets, mission, and survivability.

Incident Response

Acronis' Network Operations Center (NOC) takes the lead on incident response, identifies the root cause of a problem, and contacts the appropriate internal incident response team to triage the technology incident. The incident response team is comprised of a carefully selected group that may include representatives from our Information Security Department, Data Center Operations, Architecture and Product Development teams, as well as our Public Relations and Communications teams.

All response times are driven by internal SLAs targeted to meet 99.99 percent availability.

Acronis has developed several different escalation paths based on the type of incident and its severity. Global or high-severity level incidents are escalated directly to Acronis' executive staff.

Acronis' incident management culture is based on global best practices. There are seven stages for handling every incident:

1. **Preparation:** The organization educates users and IT staff after every incident and new implementation and trains them to respond to incidents quickly and correctly.
2. **Identification:** The team is activated and decides whether an event is, in fact, an incident. (Information about the incident can come from Acronis' monitoring system or through communication channels from different teams and customers.)
3. **Containment:** The team determines the impact, coverage of the problem, and the affected systems and customers.

4. **Eradication:** The team investigates to discover the origin of the incident, the root cause of the problem, and begins the triage process.
5. **Recovery:** The team monitors every environment for any sign of weakness or recurrence.
6. **Lessons learned:** The team analyzes the incident and how it was handled, making recommendations for preventing a re-occurrence and a plan for future response.
7. **Notification:** Internal and external communications ensure all teams and customers understand the impact and resolution steps and are apprised of status during an incident, every hour or at every significant state of change. Notifications are critical and accompany all stages of incident triage.

System & Services Acquisition

To comply with the best international practices and standards, Acronis has and continues to develop partnerships with the best data center providers to house our products and infrastructure.

Acronis Data Center partners currently have the following certifications:

Country	City	SSAE 16 Type 1	SSAE 16 Type 2	PCI DSS	ISO	ISO 9001	ISO 50001	MTCS	Tier III Uptime Institute-Design	Tier III Uptime Institute-Facility
Russia	Moscow			✓		✓			✓	✓
UK	London			✓	✓	✓				
Germany	Frankfurt	✓	✓	✓	✓	✓				
Japan	Tokyo		✓	✓	✓					
USA	Ashburn, VA	✓	✓		✓					
USA	Dallas, TX	✓	✓		✓					
Switzerland	Lupfig				✓		✓		✓	
France	Strasbourg				✓					
Germany	Frankfurt			✓	✓		✓			
USA	St. Louis, MO		✓							
Australia	Sydney		✓		✓			✓		
Singapore	Singapore				✓			✓		
Japan	Nagano				✓					

Conclusion

Acronis Cloud Data Centers are designed to meet — and exceed — the corporate and regulatory requirements of its customers. Acronis customers enjoy peace of mind knowing that Acronis is safeguarding their data and that the Acronis team is on standby 24x7x365 to address any security issues.

About Acronis

Acronis sets the standard for hybrid cloud data protection through its backup, disaster recovery, and secure file sync and share solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete, and affordable data protection of all files, applications, and operating systems across any environment — virtual, physical, cloud, and mobile.

Founded in 2003, Acronis protects the data of over five million consumers and 500,000 businesses in over 150 countries. With more than 100 patents, Acronis products have been named best product of the year, and cover a range of features, including migration, cloning and replication. Today, Acronis solutions are available worldwide through a global network of service providers, distributors, and cloud resellers.

For additional information, please visit Acronis Partner Portal at **http://partners.acronis.com**

Acronis