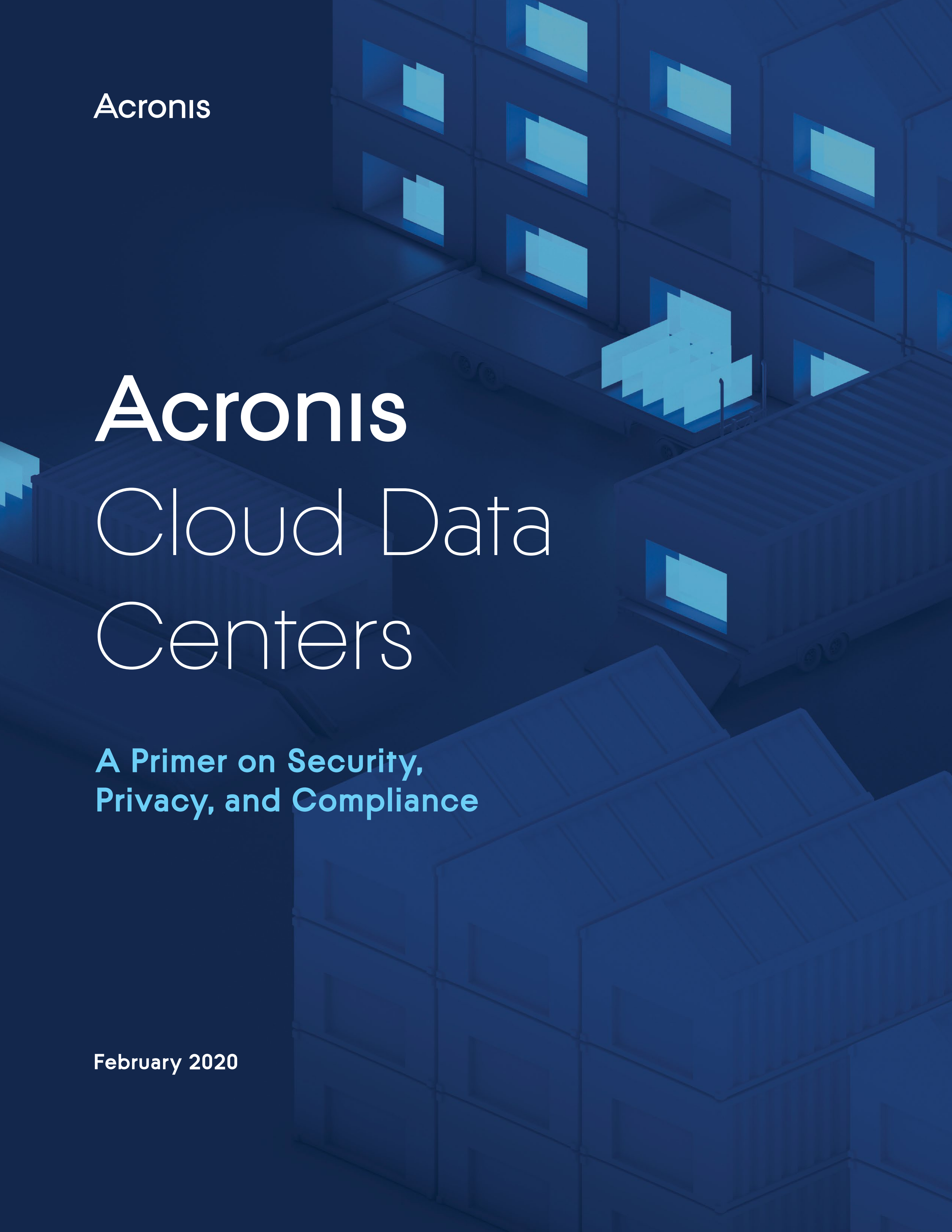

Acronis Cloud Data Centers

A Primer on Security, Privacy, and Compliance

February 2020

Table of Contents

Introduction

Since 2003, Acronis has offered industry-leading backup and disaster recovery solutions to businesses of all sizes. Today, a lot of government, financial, 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 all over the world.

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, by using their own resources. This document describes Acronis' stringent privacy and data security policies and practices regarding the confidentiality, integrity, and availability 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 and compliance program

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 and software practices. Information security is not just a steady set of strategies for managing processes, tools, and policies. Rather, information security is an ongoing process. That's why Acronis maintains a comprehensive information security and compliance program that includes administrative, physical, and technical controls based on ongoing risk assessment. Acronis information security policies and processes are based on broadly accepted international security standards such as ISO 27001 and the National Institute of Standards and Technology (NIST), and take into account the requirements of related local regulation frameworks such as Europe's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA).

Acronis has invested considerable resources to provide enterprise-level security to Acronis customers at a fraction of the cost of other on-premise and cloud information security solutions. Acronis continuously works to improve asset tracking, asset profiling, access control, and vulnerability management to provide consistent services and maintain a decent level of security. Acronis actively seeks compliance with additional guidelines and standards. 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.

To ensure the proper implementation of the information security and compliance program, Acronis continually monitors and conducts internal and external audits of compliance with the established requirements for information security and data processing. This allows Acronis to adequately measure the degree of implementation of the program and to detect and respond to the emergence of new information security risks in a timely manner.

Infrastructure and network security

Acronis hosts data and cloud products at trusted geographically-distributed data centers in the U.S., U.K., Canada, Switzerland, France, Germany, Japan, Singapore, and other locations. Customers maintain the right to choose and control which region or data center stores their data, making it easy to ensure compliance with regional requirements for data placement, as in the case of GDPR.

To confirm the reliability of data centers and ensure support for various certifications, Acronis data centers are audited regularly by respected, independent organizations. Standards and reports include:

- ISO/IEC 27001
- ISO/IEC 22301
- ISO/IEC 9001
- SSAE 16, Types 1 & 2
- Industry standards (PCI DSS, HIPAA)

The data centers employ the highest standards of physical security to restrict unauthorized physical access and protect the safety of customer data. Only authorized personnel have access to the data centers, based on strict access management, control protocols, and monitoring by surveillance cameras (CCTV). The level of protection from intruders exceeds anything that small to medium businesses can hope to implement alone.

Electrical power systems of the data centers are designed to provide uninterrupted power supply to the entire infrastructure 24 hours a day, seven days a week. The data centers are powered by at least two independent power sources. The use of automatic uninterruptible power supplies protects against power surges in case of switching power lines and provides power support during the switchover to diesel generators.

High-availability and redundant infrastructure are designed to minimize associated risks and eliminate single points of failure. 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.

This redundant infrastructure allows Acronis to fulfill most types of preventives and maintenance without service interruption. Scheduled maintenance and change to the infrastructure are carried out in accordance with the manufacturers' specifications and internal documented procedures. 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.

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.

The Acronis network is multi-layered and zone-based. The managed network equipment separates and isolates internal, external and customers' environments, and provides routing and filtering of network protocols and packets.

Acronis provides real-time encryption for all data transferred among customers and data centers, among Acronis employees and data centers and among the data centers. This real-time encryption provides the best protection for network interaction and prevents unauthorized access to the transmitted data.

Acronis uses HTTPS (TLS) secure data transfer protocols with crypto-strong encryption algorithms and provides security of cryptographic key exchange (Diffie-Hellman) to protect the transmitted data and reduce the risks of compromised key information.

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.

To ensure network security and minimize the risks of external penetration, Acronis uses the most modern web application firewalls (WAF), which include instant protection against SQL injection, cross-site scripting, unauthorized resource access, remote file inclusion, and other Open Web Application Security (OWASP) threats.

Data storage security

Acronis Cloud environment is a multi-tenant environment, so the architecture of the Acronis cloud services provides physical and logical isolation and separation of Customers' data to ensure processing of the minimum amount of data in accordance with the stated processing purposes.

Acronis stores customer data employing its own software-defined storage solution, Acronis Cyber Infrastructure with Acronis CloudRAID technology. Acronis Cyber Infrastructure delivers fast, universal, protected, efficient, and proven storage that unites block, file, and object workloads.

Acronis Cyber Infrastructure 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 Cyber Infrastructure 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. At the same time, the unique flexibility and scalability of Acronis Cyber Infrastructure ensures this exponential rate of growth does not affect customer critical data in any way.

Acronis Cyber Infrastructure drives and equipment on which the data storage and/or processing are carried out can be broken, switched out for repair, or decommissioned. In these cases, Acronis takes measures aimed at a complete erasure of data from disks and the removal of residual data from the internal memory of the equipment according to NIST SP 800-88rev1. In the event that it is not possible to erase (delete) such information, physical destruction of equipment is performed in a way that makes it impossible to read (restore) such data.

Personnel security

Maintaining data security is impossible without people. Despite the fact that the personnel are the most important asset, Acronis understands that a main security concern also relates to 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 Acronis personnel are obligated to comply with Acronis' confidentiality, business ethics, and code of conduct policies. Acronis pays special attention to the selection of personnel by conducting appropriate background verification checks on candidates for employment in accordance with applicable local laws, statutory regulations, and ethics. Every Acronis employee is required to sign a Non-Disclosure Agreement (NDA).

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.

All employees receive awareness education and training regarding information security, privacy protection, and data processing, as is appropriate relative to their job functions and assigned roles.

Access control

Acronis has implemented an enterprise-wide access control policy to restrict access to information resources and data in accordance with official duties. Access provisioning is based on the Need to Know and Least Privileges principles.

Internal access control procedures detect and prevent unauthorized access to Acronis systems and information resources. When providing access, Acronis uses centralized access control systems with secure mechanisms and authentication protocols (LDAP, Kerberos, SSH certificates), unique user IDs, strong passwords, two-factor authentication mechanisms, and limited control access lists to minimize the likelihood of unauthorized access.

In addition, any access is recorded in system audit logs, changes to which are not allowed. The audit logs are periodically reviewed.

Software practices

Acronis uses the latest versions of software and regularly updates its operating systems, software, frameworks, and libraries. 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 according to their jobs and roles.

Incident management

Acronis' Network Operations Center (NOC) takes the lead on incident identification and 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 and Compliance 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.

Business continuity and disaster recovery

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 risk and business impact analysis at all Acronis locations.

Acronis maintains Business and Disaster Recovery Program in place that addresses its critical processes and technology at all its data centers. Acronis periodically tests and updates of its internal Business Continuity and Disaster Recovery Plans to ensure adequate reaction and availability of its services in case of potential disruptive events occur.

Testing of disaster recovery plans is conducted at least once a year, according to the scenarios of the most potential threats in relation with particular assets. At the same time, the testing scenarios are coordinated with regard to stopping the provision of the service in consequence of various threats determined by those responsible for performing the service. The testing plans are approved for a year by the Information Security Committee and can be carried out in one of the following ways:

- Checklist
- Structured walk-through
- Simulation
- Interruption

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 strong requirements for data center locations to reduce or completely eliminate probability of the most natural of disruptive events.

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
- Protect Acronis' assets, mission, and survivability

Supplier relationship management

Before contracting with any third-party subprocessor, data center, or service provider, Acronis conducts a thorough diligence process to ensure each third party can provide an appropriate level of security and privacy corresponding to the level of data access. Contracts with third parties contain information security, privacy, and confidentiality requirements. During the term of each contract, Acronis regularly monitors and reviews the third party's security controls, service delivery and compliance with contractual requirements.

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 leads the world in cyber protection – solving safety, accessibility, privacy, authenticity, and security (SAPAS) challenges with innovative backup, security, disaster recovery, and enterprise file sync and share solutions that run in hybrid cloud environments: on-premises, in the cloud, or at the edge. Enhanced by AI technologies and blockchain-based authentication, Acronis protects all data, in any environment, including physical, virtual, cloud, mobile workloads and applications.

With 500,000 business customers, and a powerful worldwide community of Acronis API-enabled service providers, resellers and ISV partners, Acronis is trusted by 100% of Fortune 1000 companies and has over 5 million customers. With dual headquarters in Switzerland and Singapore, Acronis is a global organization with offices worldwide and customers and partners in over 150 countries. Learn more at acronis.com

For additional information, please visit www.acronis.com