Acronis

WHITE PAPER

Two guidelines from three ministries (2G3M)

Table of contents

Introduction

Since 2003, Acronis has offered industry-leading backup and disaster recovery solutions to businesses of all sizes. Today, numerous government, financial, medical and other organizations with extreme data sensitivity and robust security requirements, as well as 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 operating within a variety of business sectors. This white paper describes Acronis' fulfillment of its obligations and delineates how customers can use Acronis Cyber Protect Cloud to fulfill their own obligations in handling medical information according to Japanese government requirements.

In Japan, systems that process and / or store personally identifiable medical information (Medical PII) must adhere to two key guidelines:

- The Guideline for Safety Management of Medical Information Systems[1].
- The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information[2].

Together, these guidelines are commonly known as the '2 Guidelines from 3 Ministries' (2G3M). Acronis is dedicated to supporting our customers in fulfilling their obligations under 2G3M. We provide a secure foundation for building systems, offer tools to enhance system security, and offer educational resources to help our customers maximize the utility of these tools.

Compliance with 2G3M standards in Japan is primarily driven by voluntary self-regulation among health care providers, although serious violations may incur administrative penalties.

This white paper serves informational purposes only. It does not constitute legal advice, and readers should seek professional legal guidance for any specific concerns regarding compliance with 2G3M or other regulations.

Requirements

Scope

The Guideline for Safety Management of Medical Information Systems encompasses a broad range of entities, including hospitals, clinics, maternity homes, pharmacies, home-visit nursing stations, care providers and medical information networks. It delineates compliance requirements for users of systems handling medical personally identifiable information (PII) and serves as the cornerstone of regulatory compliance in Japan's health care sector.

The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information outlines specific compliance requirements for entities providing systems and services that handle digitized medical PII. It serves as framework for ensuring the secure design, implementation and operation of information

[1] Guidelines for safety management of medical information systems Version 6.0 released in 2023, https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

[2] Safety Management Guideline for Information Systems and Service Providers Handling Version 1.1 released in 2023, https://www.soumu.go.jp/main_content/000891033.pdf

systems and services utilized in health care settings, including cloud-based services like Acronis Cloud, when it is integrated into such infrastructures.

Risk management measures

The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information requires service providers to engage in both risk management and risk communication.

Regarding risk management, the guideline requires that service providers must delineate information flows, identify and assess risks, and implement appropriate risk management measures. Because the information flows differ for each Acronis user, it is difficult to present the response for each situation. Therefore, Acronis drafted a compatibility matrix in accordance with the “Attachment 2 List of countermeasure items in preintegration guidelines and correspondence table of medical information safety management guidelines version 6.0." Other than the numbering adopted by the aforementioned Attachment 2 and the relative “content of the requirement” is added how Acronis complies with them, as well as a map with the ISO/IEC 27000 family certifications held by Acronis.

Risk management measures required to fulfill all these requirements have been designed with the following three perspectives in mind:

❶ **Human and organizational**. These controls are related to organizational security and personnel security.

- **Organizational security**: Involves establishing, operating and documenting an organizational structure to oversee security management.
- **Personnel security**: Ensures that staff members uphold confidentiality and receive training on security posture.

❷ **Physical**. This involves implementing physical access controls such as barriers and locks, along with related measures to regulate facility access.

❸ **Technical**. This encompasses digital access controls, including authentication, authorization and access controls, as well as additional security measures such as logging, encryption, data leak prevention, vulnerability management and threat detection.

Concerning risk communication, providers are obliged to disclose their risk management strategies to medical institutions. This involves clarifying the steps medical institutions can take to mitigate risk when utilizing their services.

Shared responsibility model

Acronis has the responsibility to assure security of its own cloud infrastructure, including vendor selection, while their customers have the responsibility to secure their own environment.

Shared with colocated data centers

Physical security for colocated data centers is a responsibility shared with each data center facility.

Acronis has established partnerships that run numerous global, colocated data center facilities. These facilities meet rigorous standards and compliance needs regarding setup, power and cooling. This approach maintains optimal conditions and uptime to safeguard mission-critical data. Additionally, Acronis has strict requirements for data centers to reduce or eliminate the probability of the most typical disruptive events. During the term of each contract, Acronis regularly monitors and reviews the third party’s security controls, service delivery and compliance with contractual requirements.

Shared with customers

Acronis as a company differentiates between two types of data:

- Data necessary for providing the services (e.g., product usage) and Acronis' service management. This is the data that Acronis collects and processes as a data controller for providing our services. Such data may include account names, email and other contact details, billing details and some information automatically collected via the service, which may be personal in nature. For more details, please check the Acronis Privacy Statement: https://www.acronis.com/company/privacy/
- Customers' content data. This is the data that Acronis may process as a data processor (subprocessor) when you use our services. The information is provided by customers while utilizing specific products (e.g., backup archives, files, virtual machines, etc.). In terms of this type of data, Acronis does not control the categories and the content of the information customers are storing with us.

Customers are solely responsible for evaluating and maintaining their own legal, compliance and technical obligations. As Acronis does not know what data may be provided as part of the content data, customers should confirm with Acronis when they have to meet some specific requirements. Acronis can sign a standard Data Processing Agreement with with the customers who have such obligations under applicable data protection regimes.

Organizational security measures

Requirement	Acronis
Holding Privacy Mark certification or ISMS certification.	• Information Security and Compliance Program. • Security assurance to 2G3M.
Confirming that the equipment or devices used for storing information are subject to domestic law.	• Data protection. • Infrastructure and network security.
Regular verification of the location of equipment and media.	• Infrastructure and network security. • Data storage security. • Access control.
Clarification of roles and responsibilities with medical institutions.	• Shared responsibility model. • Information Security and Compliance Program. • Data protection.
Monitoring of access and manipulation activities within medical information.	• Infrastructure and network security. • Personnel security. • Access control.
Personally identifiable information (PII) secure processing and handling.	• Data protection. • Information Security and Compliance Program. • Access control.
Implementation of internal audits.	• Information Security and Compliance Program. • Security assurance to 2G3M.
ICT supply chain security management.	• Supplier relationship management. • Application security. • Data protection. • Incident management.
Business continuity plan development.	• Business continuity and disaster recovery. • Incident management.
Response to incidents caused by cyberattacks, including reporting to medical institutions.	• Incident management. • Personnel security. • Business continuity and disaster recovery. • Infrastructure and network security.
Quality management of equipment and software.	• Application security. • Incident management.
Minimizing the impact on medical institutions associated with changes.	• Infrastructure and network security. • Application security. • Access control.

Personnel security measures

Requirement	Acronis
Contract engagement of confidentiality obligation with all staff.	• Personnel security. • Supplier relationship management.
Implementation of education and training related to the provision of medical information systems and similar services.	• Personnel security. • Incident management.
Implement security measures and supervise employees and subcontractors.	• Supplier relationship management. • Personnel security.

Physical security measures

Requirement	Acronis
Access control management.	• Access control. • Infrastructure and network security. • Information Security and Compliance Program.
Measures against equipment theft.	• Infrastructure and network security. • Access control.
Measures against earthquakes, floods, lightning, fires and related power outages.	• Supplier relationship management. • Personnel security.
Secure media disposal.	• Data storage security. • Infrastructure and network security.

Technical security measures

Requirement	Acronis
Implementation of user authentication.	• Access control. • Infrastructure and network security.
Access rights management.	• Access control.
Log acquisition and verification.	• Incident management. • Access control. • Application security. • Endpoint security.
Measures against malicious programs.	• Endpoint security. • Incident management.
Hardening and updates of terminals and servers.	• Endpoint security. • Infrastructure and network security. • Application security.
Vulnerabilities management.	• Application security. • Information Security and Compliance Program.
Network access control.	• Infrastructure and network security. • Access control.
Restriction of unregistered electronic media connections.	• Endpoint security.
Use of encryption and electronic signatures.	• Infrastructure and network security. • Data storage security. • Access control.
Management of backup and restoration.	• Endpoint security.

Acronis Cyber Protect Cloud security

Acronis maintains a comprehensive Information Security and Compliance Program that includes human, organizational, physical and technical controls based on ongoing risk assessments. Acronis information security policies and processes are based on broadly accepted international security standards such as the ISO/IEC 27000 series or the National Institute of Standards and Technology (NIST), and take into account the requirements of related local regulation frameworks such as Japan's Act on the Protection of Personal Information (APPI) and the European Union (EU) General Data Protection Regulation (GDPR).

Information Security and Compliance Program

We look at information security not just as a steady set of strategies for managing processes, tools and policies, but also as an ongoing process with multiple players, where the role of the individual matters and the key role player is information.

The Acronis Information Security Management System (ISMS) has been certified by independent third-party auditors in accordance with the ISO/IEC 27001 framework for information security, which has become an industry gold standard. To answer to the cloud demands for security on top of legacy systems, we extended and certified our ISMS with ISO/IEC 27017 for cloud security practices and ISO/IEC 27018 to assure the security of personally identifiable information (PII) in the cloud.

In order to provide further assurance about our security practices, Acronis has also pursued obtaining the System and Organization Controls 2 (SOC 2®) Report for Service Organizations. This standard applies trust services criteria and requirements for organizations that manage customers' data.

We also consider our customers' demands related to local privacy and data protection regulations such as Japan's Act on the Protection of Personal Information (APPI), Europe's General Data Protection Regulation (GDPR), United States' Health Insurance Portability and Accountability Act (HIPAA), France's Health Data Hosting (HDS), etc.

Acronis has invested considerable resources to guarantee enterprise-level security for its customers at a fraction of the cost of other on-premises and cloud information security solutions. Acronis continuously

works to improve asset tracking, asset profiling and access control and vulnerability management to ensure consistent services and maintain a decent level of security. Acronis actively seeks compliance with well-known information security standards and accepted best practices. All our information security measures are integrated and coordinated with the Acronis Business Continuity Management Program to minimize any security threat and natural and human-made hazards.

To ensure the proper implementation of the Information Security and Compliance Program, Acronis continually monitors and conducts internal and external audits to verify compliance with established requirements for information security and data processing. This enables Acronis to adequately measure the degree of our program implementation and to detect and respond to the emergence of new security risks.

Security assurance to 2G3M

The most relevant third-party certifications for Acronis customers who need to comply with 2G3M are:

ISO/IEC 27001 An internationally recognized standard that sets out the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). It provides a systematic approach to identifying, assessing and managing information security risks, helping organizations to safeguard their data and protect against potential security threats. It emphasizes the importance of a risk-based approach, requiring organizations to tailor their information security controls to their specific business needs and risk profile.

Acronis' compliance with ISO/IEC 27001 is crucial to demonstrate our commitment to information security best practices, instilling trust and confidence in clients. It provides a structured framework for managing sensitive data and mitigating security risks, thereby enhancing the company's credibility and reputation in the industry. Adhering to this standard helps Acronis ensure the confidentiality, integrity and availability of client information, fostering long-term relationships built on trust and reliability. Furthermore, ISO/IEC 27001 compliance enables Acronis to stay ahead of evolving cybersecurity threats, ensuring continual improvement and adaptability in the face of emerging challenges.

ISO/IEC 27017 provides valuable guidance specifically tailored to cloud service providers, offering a framework for implementing effective cloud security measures. By aligning with this standard, Acronis demonstrates its commitment to safeguarding cloud-based data and services, instilling confidence in clients who rely on cloud solutions.

ISO/IEC 27018 provides comprehensive guidelines for cloud service providers like Acronis, ensuring the privacy and protection of personal information stored and processed in the cloud. By embracing this standard, Acronis showcases its dedication to safeguarding the privacy rights of individuals and complying with relevant data protection regulations.

The SOC 2 Type II report is a comprehensive assessment conducted by an independent auditor to evaluate a cloud service provider's internal controls related to security, availability, processing integrity, confidentiality and privacy. It verifies whether these controls are designed effectively and operating efficiently over a specified period — typically six to twelve months.

By obtaining an SOC 2 Type II report, Acronis demonstrates its commitment to maintaining robust security practices and ensuring the availability, integrity and confidentiality of client data.

Infrastructure and network security

Acronis hosts data and cloud products at trusted and geographically distributed data centers in the U.S., U.K., France, Germany, Japan, Singapore, Switzerland and multiple other locations, as displayed on our website (https://www.acronis.com/data-centers/).

Customers can choose which region or data center to store their data, making it possible to ensure compliance with regional requirements for data placement, as in the case of GDPR, APPI (required by 2G3M) and other local privacy and data protection regulations.

When selecting our data center providers and their locations, we thoroughly assess providers taking into account the capabilities of the facility, the current evaluation of the threats (constructional, technical, environmental, political, etc.), and the relative attractiveness of and business requirements for the specific region.

To confirm the reliability of data center providers and ensure their capability to maintain the security, availability, confidentiality and integrity of information, our data center providers are audited regularly by respected independent organizations.

Acronis demands that 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 control measures and monitoring by surveillance cameras (CCTV). The level of protection from intruders exceeds anything that small to medium-sized businesses can hope to implement alone.

The electrical power systems in these data centers are designed to provide an uninterrupted power supply to the entire infrastructure 24 hours a day, 7 days a week. The data centers are powered by at least two independent power sources. The use of automatic, noninterruptible power supplies protects against power surges in the case of switching power lines, and provides power support during switchovers to diesel generators.

High availability and redundant infrastructures 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 either the Acronis critical infrastructure or Acronis customers.

This redundant infrastructure allows Acronis to fulfill most types of preventive and maintenance activities without service interruption. Scheduled maintenance and changes to the infrastructure are carried out in accordance with the manufacturers' specifications and internal documented change management procedures. Every piece of equipment is under warranty and all elements of the infrastructure are covered under each respective vendor's SLA. A dedicated team manages all vendor maintenance contracts, which are subject to annual 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 about new or existing vulnerabilities. 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 any issues that may arise.

Acronis commissions security audits from third parties to verify that all components and configurations are free from security issues.

Acronis performs daily scans of critical infrastructure and regularly checks the configuration of all network security components.

Acronis reviews the security of new services and the architecture of network interaction with these services before integrating them into the company's network.

The Acronis network is multilayered 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. Acronis utilizes secure data transfer protocols (HTTPS, TLS, SSH, OpenVPN, etc.) with crypto-strong encryption algorithms, and provides security of cryptographic key exchange (Diffie-Hellman, RSA) to protect the transmitted data and reduce the risks of unauthorized access to the transmitted data and compromised key information.

Acronis continuously monitors the security of its entire IT infrastructure to protect against advanced persistent threats (APTs) and cyberattacks. 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 intervention.

To safeguard against SQL injection attacks, we use an exclusively prepared statements library for all our database queries. This approach ensures that a user's input is safely parameterised, preventing any unauthorized manipulation of our SQL commands. Additionally, our custom-built, client-side framework is designed with built-in protection against cross-site scripting (XSS) attacks.

This framework automatically exposes unsafe characters, ensuring that any potentially harmful scripts are neutralised before they can be executed in the user's

browser. For ensuring that users can access only the data they are authorized to view, we have developed an internal server-side component that rigorously enforces data access controls based on a unique tenant model.

This tenant model ensures that each user's access is strictly limited to their assigned scope, preventing unauthorized access to data which belongs to other users or tenants. Every server-side component within our system is required to call this central authority to resolve permissions, ensuring consistent and secure data handling across our entire platform.

Data protection

Global privacy developments pose a significant compliance burden on businesses — especially for those operating worldwide. Acronis is committed to complying with local data protection regulations as applicable.

The Act on the Protection of Personal Information (APPI) has regulated privacy in Japan for more than 20 years, and Acronis is committed to complying with applicable data protection regulations, including the requirements of the Japanese APPI. We design our products and services with data protection in mind. Acronis works hard to keep information secure, and we regularly monitor and update our security practices to help better protect privacy. Acronis has also developed policies and procedures for fulfilling our applicable obligations. An individual under APPI has a number of privacy rights, and Acronis will respond to and address privacy requests accordingly.

For more information on Acronis' data processing practices, you can check our Privacy FAQ and the Acronis Privacy Statement.

Data storage security

The Acronis Cyber Cloud environment is multitenant, so the architecture of our cloud services provides physical and logical isolation and separation of customers' data to ensure processing of the minimum amount of data in accordance with stated processing purposes.

Acronis stores customers' data employing its own software-defined storage solution, Acronis Cyber Infrastructure with Acronis CloudRAID technology. Acronis Cyber Cloud 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 which minimize data risks. In addition, Acronis Cyber Infrastructure utilizes a fully redundant architecture to safeguard data integrity for every customer.

All Acronis Cyber Cloud environments are encrypted at rest by the Advanced Encryption Standard (AES) with a 256-bit key.

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 Storage ensures this exponential rate of growth will 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 800-88. 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 and restore such data.

Personnel security

Maintaining data security is impossible without people. Despite the fact that personnel are an organization's most important asset, Acronis also understands that a main security concern relates to employees. No system or infrastructure can be 100% protected without establishing a corporate-wide security culture.

All Acronis personnel receive awareness education and training regarding information security, privacy protection and data processing appropriate to their job functions and assigned roles.

Acronis also 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 obligated to comply with the Acronis confidentiality, business ethics and Code of Conduct policies and is required to sign a nondisclosure agreement (NDA), which remains valid even after termination of an employment contract.

Endpoint security

Securing endpoint devices is crucial for protecting sensitive data, preventing unauthorized access and defending against cyberthreats like malware, data loss, etc. Acronis use its own solution, Acronis Cyber Protect Cloud, to protect its endpoint devices to minimize time action to:

- Close security vulnerabilities using our threat intelligence feed, forensic insights, patch management, blocking of analyzed attacks and policy management.
- Continuous monitoring for security-related events using automated behavioral and signature-based engines, URL filtering, an emerging threat intelligence feed and event correlation.
- Investigate suspicious activities and conduct follow-up audits using a secure, remote connection into workloads or reviewing automatically saved forensic data in backups.

Access control

Acronis has implemented an enterprise zero trust access control policy to restrict access to information resources and data in accordance with official duties.

For all positions, Acronis follows the principle of segregation of duties, need to know and least privilege. This ensures that every user has the least amount of privilege necessary to complete a job, and all critical operations are controlled and accountable. Only staff with the highest clearance can access data center environments.

Internal access control procedures detect and prevent unauthorised access to Acronis systems and data. When providing access, Acronis uses centralised zero trust access control systems with secure mechanisms and authentication protocols (e.g., LDAP, Kerberos, SSH certificates, 802.1x), unique user IDs, strong passwords, multifactor authentication mechanisms and limited-control access lists to minimize the likelihood of unauthorized access.

In addition, any access is recorded in system audit logs, which are protected from changes and are periodically reviewed.

On top of logical access control practices and at rest encryption, Acronis provides customers with the capability to encrypt their data based on a key generated from customers' passwords, which gives them complete control over their data.

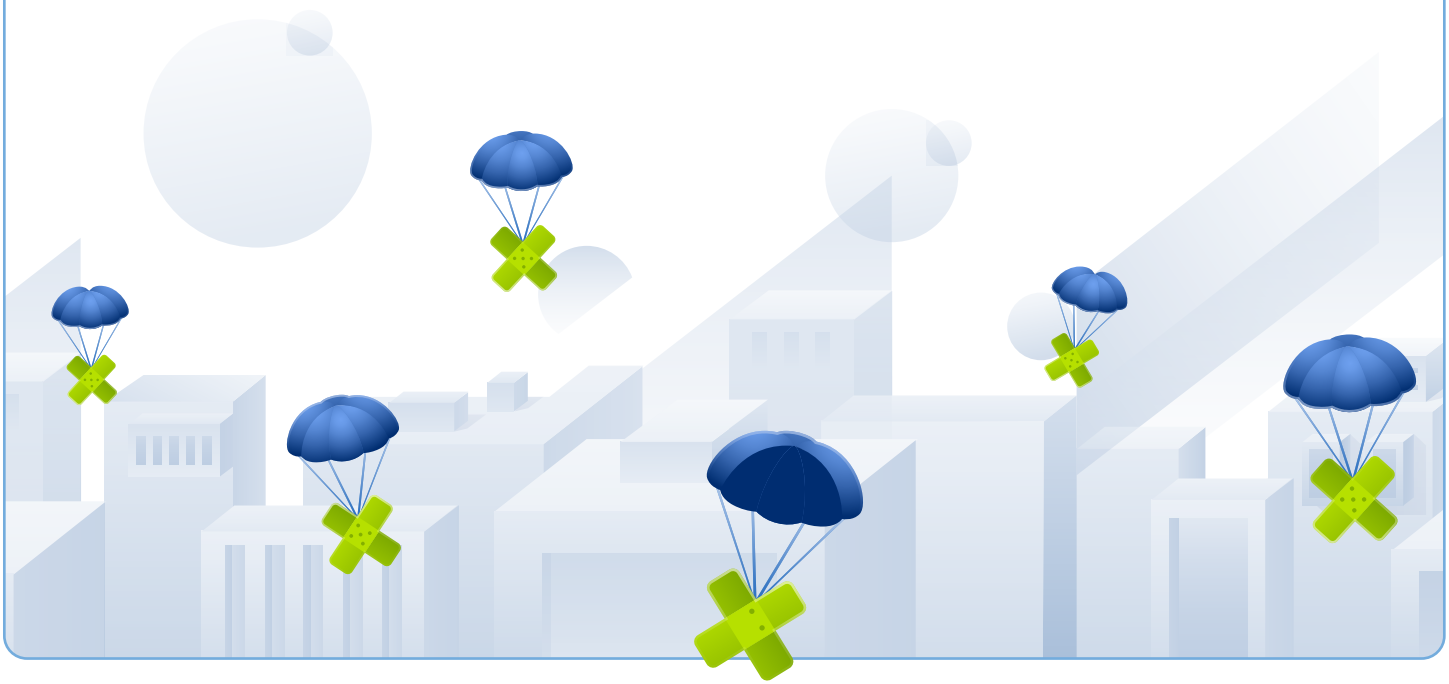
Application security

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.

Third-party components, including open-source, are cloned into an internal Acronis repository before they can be linked to the main software. All components are reviewed by development and information security teams and approved for use in the development process. Also, the company's technical leadership is informed about components to be used in software development. Security teams regularly monitor for updates issued for the components in use, and if an update contains a vulnerability fix, it will be reviewed and the internal repository will be updated.

Our standard software security practices include:

- Adherence to strict security policies and well-known security best practices to incorporate security at every stage of the secure software development lifecycle.
- Security review of architectures, design of features and final solutions. Information security and quality assurance teams perform security reviews. This includes application scanning for known vulnerabilities, opened ports, etc. And besides internal reviews, Acronis conducts external reviews performed by an independent third party.
- 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. During development, any modifications to the source code are reviewed by an expert in that particular software, and two engineers. All submitted changes are always linked to a ticket in a task management system used by Acronis.
- Code assessment by static application security testing (SAST) tools as part of the software continuous delivery (CI/CD) pipeline to ensure quick feedback to developers. The process is automated and all activities are recorded for the Acronis information security team's future audits.
- Building and constantly maintaining security culture among all teams and keeping them vigilant to known vulnerabilities and current information security threats.
- Acronis has been running a bug bounty program on HackerOne since 2018. Acronis works closely with the security community and embraces researchers who contribute toward the optimization of our products.
- As a partner of the CVE Program, Acronis is a CVE Numbering Authority (CNA) responsible for publishing disclosed cybersecurity vulnerabilities as CVE records for all Acronis products. For information on security advisories and updates, see the Acronis Security Advisory Database.



Incident management

The Acronis security operation team and 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 incident.

The incident response team is comprised of a carefully selected group that includes representatives from our security and compliance department, data center operations and architecture and product development teams, as well as our public relations and communications teams.

All response times are driven by internal service level agreement (SLA) targets (99.9% availability), and legal and contract obligations.

Acronis has developed several different escalation paths based on the type of incident and its severity. Global or high-severity-level incidents are escalated and controlled by Acronis executives.

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

Preparation: Appropriate security controls are in place and kept up to date. A well-defined incident response plan is established and communicated to all responsible teams. Provision of education for users and IT staff after every incident and new implementation and training for them to be able to respond to incidents quickly and correctly.

Identification: The network operations center (NOC) monitors for suspicious system events on a 24/7 basis. The NOC can also be supported by the security operations center (SOC) by rapidly performing an initial triage and analysis to determine whether an information security event is in fact an incident, and what its scope is — such as which networks, systems, applications, hosts or data centers are affected. The objective of the initial analysis is to provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of its effects. Information about data security events is collected through different channels and Acronis monitoring systems.

Containment: This stage is important in the course of handling each incident and before the incident overwhelms Acronis resources or customer data. The team determines the coverage of the problem, its impact and affected systems and customers. An essential part of our containment stage is decision making (e.g., for shutting down a system or disabling certain functions).

Eradication: The team investigates to discover the origin of the incident and the root cause of the problem, and begins the elimination process, such as by removing malware or disabling breached accounts. For some incidents, eradication may either not be necessary or is performed during recovery.

Recovery: Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords and tightening network perimeter security. An additional objective of the recovery phase is to prevent similar incidents in the future. For this reason, the NOC team monitors every environment for any signs of weakness or recurrence.

Lessons learned: The team analyzes the incident and how it was handled, making recommendations for preventing a recurrence and a plan for future response.

Notification: Internal and external communications ensure all teams and customers understand the impact and resolution steps undertaken, and are apprised of status at every significant stage of the incident triage.

Business continuity and disaster recovery

Many potential disruptive threats can occur at any time and any location, adversely affecting business operations. Acronis considers a wide range of potential threats as part of risk and business impact analysis at all Acronis locations (offices and data centers), including critical processes and systems.

Acronis recognizes the importance of having a comprehensive business continuity and disaster recovery planning program to:

- Protect employees' 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 ensure adequate reaction and availability of its services in case potential disruptive events occur, Acronis periodically reviews and updates its internal business continuity and disaster recovery plans. Testing of disaster recovery plans is conducted at least once a year, according to scenarios for most potential threats in relation to particular assets. At the same time, these testing scenarios are coordinated with regard to stopping the provision of the service as a 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:

- Checklists
- 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 disruptive events.

Acronis does not currently perform backup of backups. Acronis instead utilizes redundant infrastructure to eliminate single points of failure. Our backup strategy and disaster recovery plans are focused on service recovery.

Acronis requires the commitment of each employee, department and vendor to:

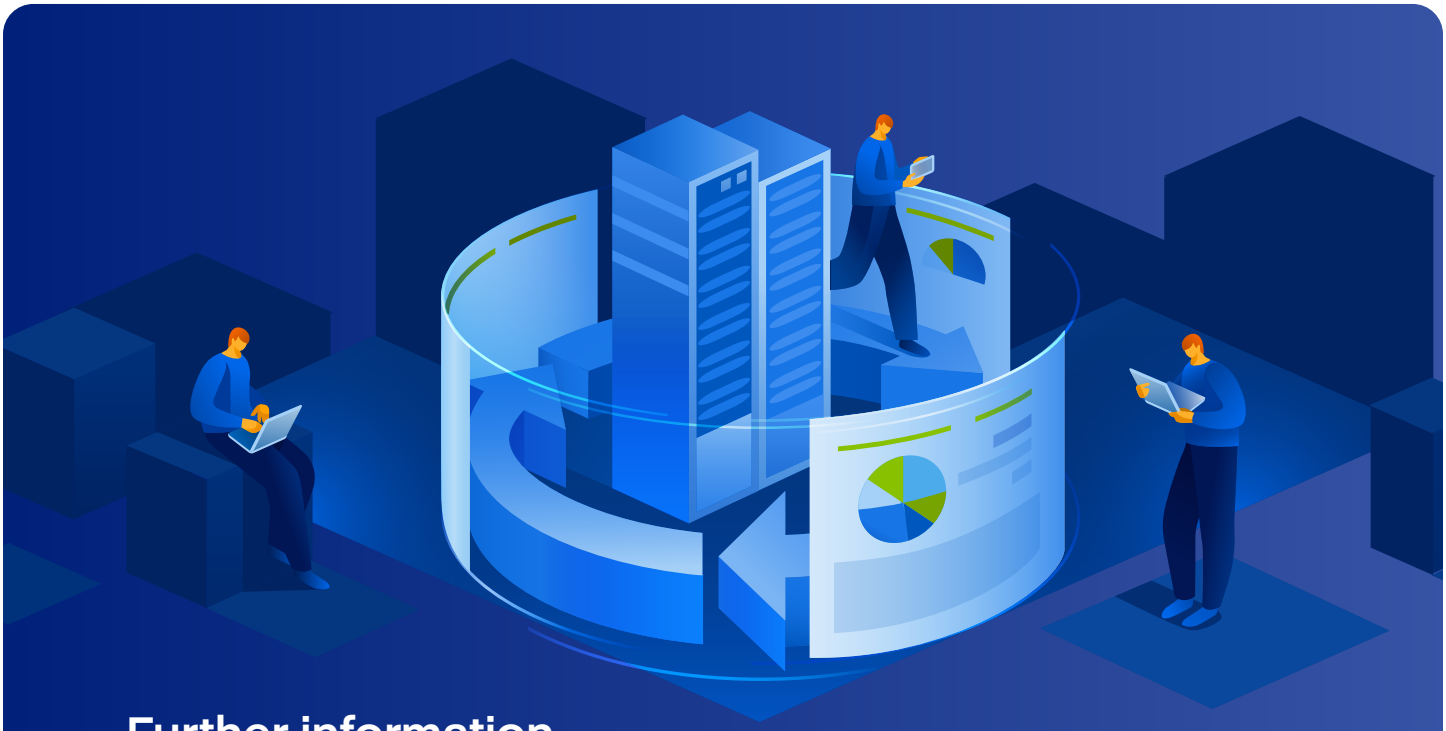
- Support its business continuity program objectives.
- Review, build, test and grow its business continuity and disaster recovery program.
- Protect Acronis' assets, mission and survivability.

Supplier relationship management

Suppliers are an integral part of any business. However, no matter how well your assets are protected within the company, when attracting third parties, you must make sure that they are reliable.

The Acronis vendor selection process begins with defining criteria for the third party. Along with business requirements, we consider both our security and data protection requirements, as well as our customers' requirements.

Before contracting with third-party subprocessors, data centers or service providers, Acronis conducts a thorough vendor assessment to ensure that third parties can provide an appropriate level of security and privacy corresponding to the level of data access. Contracts with third parties contain information about security, privacy and confidentiality requirements, and during the term of each contract, Acronis regularly monitors and reviews the third party's security controls, service delivery and compliance with contractual requirements.



Further information

For more information on Acronis' cybersecurity and compliance posture, please refer to:

TRUST CENTER PRIVACY LEGAL