DATA COMPLIANCE & CERTIFICATIONS

any.cloud

IBM Platinum Partner

Compliance commitment

The purpose of this document is to inform Anycloud A/S's distributors, partners and auditors about the requirements listed in the international standard for assurance engagements regarding assurance reports on controls at a service organization. Anycloud is an ISO 27001 certified company with an SLA formed by the regulations and requirements based on ISO 27001. Anycloud is a certified member of the Cloud Security Alliance (CSA STAR) and has an ISAE 3000 assurance report made by an independent external auditor every year. We are committed to be an international vendor of leading cloud SaaS offerings delivered with simplicity and scalability, and therefore a data processing agreement is always part of our service.

VIEW OUR DATA PROCESSING AGREEMENT

Certifications

ISO 27001
CERTIFIED

Anycloud is certified within the ISO 27001 standard. Working with the framework of standards in how to manage information and data. As a cornerstone in Anycloud's business, risk-management is key to all actions Anycloud performs.

Download report

ISAE 3000
ASSURANCE REPORT

Anycloud holds an independent auditor's report. The ISAE 3000 is a control report that controls Anycloud under the ISO 27001 and 27002 standards. This generates a fully public report that confirms Anycloud's actions and internal processes.

Download report

CLOUD SECURITY
ALLIANCE

The membership of CSA is an addition to the official certifications and auditing reports. By being a member of CSA Anycloud holds an CAIQ – a questionnaire that answers most security and compliance questions that Anycloud partners and customers has.

Download report

Security standards

We are committed to the security and privacy of our partners, distributors, and their customers. We strive to implement and maintain security processes, procedures, standards, and take all reasonable care to prevent unauthorized access to customer data. We apply appropriate administrative, operational, and technical security controls to help ensure that customer data is handled and processed in a responsible and secure manner.
We prioritize the implementation of robust security measures to safeguard against cyber threats and vulnerabilities.

Regulatory compliance

We adhere to industry-leading security standards and have an ISO 27001 certification and ISAE 3000 assurance report made by an independent external auditing company every year. The report controls Anycloud under the ISO and GDPR legislation. This generates a fully public report that confirms and certifies Anycloud's actions and internal processes.
Anycloud is also a certified member of the Cloud Security Alliance (CSA STAR). The membership of CSA is an addition to the official certifications and auditing reports. By being a member of CSA Anycloud holds an CAIQ – a questionnaire that answers most security and compliance questions that Anycloud partners and distributors have.

Security standards

We are committed to the security and privacy of our partners, distributors, and their customers. We strive to implement and maintain security processes, procedures, standards, and take all reasonable care to prevent unauthorized access to customer data. We apply appropriate administrative, operational, and technical security controls to help ensure that customer data is handled and processed in a responsible and secure manner.
We prioritize the implementation of robust security measures to safeguard against cyber threats and vulnerabilities.

Security statement

Anycloud is committed to the security and privacy of our partners, distributors, and their customers. We strive to implement and maintain security processes, procedures, standards, and take all reasonable care to prevent unauthorized access to customer data. We apply appropriate administrative, operational, and technical security controls to help ensure that our customer data is handled and processed in a responsible and secure manner. This Security Statement is aimed at providing you with more information about our security infrastructure and practices.

Information Security Policy

Anycloud maintains a written Information Security policy that defines employee responsibilities and acceptable use of information system resources. The company receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior before providing authorized access to Anycloud information systems. This policy is reviewed annually and updated as necessary.
Our comprehensive security policies cover a diverse range of security related subjects including but not limited to general standards with which every employee must comply, such as account, data, and physical security, to more specialized security standards covering internal applications and information systems.

Organizational Security

Information security roles and responsibilities are defined within the organization. The Anycloud security department focuses on information security, global security auditing and compliance, as well as defining the security controls for protection of Anycloud's hardware and cloud infrastructure. The team receives information system security notifications on a regular basis and distributes security alert and advisory information to the organization on a routine basis after assessing the risk and impact as appropriate.
Anycloud adheres to the International Organization for Standardization (ISO) 27001 Framework employing a multi-layered security control approach to identify, prevent, detect, and respond to security incidents. The security team is also responsible for tracking incidents, vulnerability assessments, threat mitigation, and risk management.

Asset Management

Anycloud data and information system assets are comprised of partner, distributor, and end-user assets as well as corporate assets. These asset types are managed under our security policies and procedures. Anycloud authorized personnel are trained to understand how these assets contribute to our overall security posture and trained to comply with the policies and procedures when procuring and managing them.

Personnel Security

Anycloud employees are required to conduct themselves in a manner consistent with the company's guidelines, including those regarding confidentiality, business ethics, appropriate usage, and professional standards. All newly hired employees are required to sign confidentiality agreements and to acknowledge Anycloud policies. The policies outlines the company's expectation that every employee will conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors. Processes and procedures are in place to address employees who are on-boarded and off-boarded from the company.
Employees are provided with security training as part of new hire orientation. In addition, each Anycloud employee is required to read, understand, and take training courses twice a year for security, avoidance of breaches and data protection.

Physical and Environmental Security

Anycloud has policies, procedures, and infrastructure to handle both the physical security of its datacenters as well as the environment from which the datacenters operate. Our information systems and infrastructure are hosted in datacenters that are geographically dispersed to provide high availability and redundancy to Anycloud and its partners and distributors. The standard physical security controls implemented at each data center include electronic card access control systems, fire alarm and suppression systems, interior and exterior cameras, and security guards. Physical access is centrally managed and strictly controlled by data center personnel. All visitors and contractors are required to present identification, are required to log in, and be escorted by authorized staff through the data center.

Access to areas where systems or system components are installed or stored are segregated from general office and public areas. The cameras and alarms for each of these areas are centrally monitored 24/7 for suspicious activity, and the facilities are routinely patrolled by security guards. Servers have redundant internal and external power supplies. Datacenters have backup power supplies and can draw power from diesel generators and backup batteries. These datacenters have undergone SSAE 16 audits, which produced a Service Organization Control (SOC) 2 Type II attestation letters. Furthermore, the datacenters are ISO 27001 certified.

Operational Security

Change Management

Anycloud maintains a change management process to ensure that all changes made to the production environment are applied in a deliberate manner. Changes to information systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested, and monitored post-implementation to ensure that the expected changes are operating as intended.

Supplier and Vendor Relationships

Anycloud collaborates with suppliers and vendors that operate with the same or similar values around lawfulness, ethics, and integrity that Anycloud does. As part of its review process, Anycloud rigorously assess our suppliers and vendors and bind them to uphold appropriate confidentiality and security obligations, including requirements for appropriate management of any data they may handle.

Auditing and Logging

We maintain system audit logs which provide an account of which personnel have accessed which systems. We limit access of our auditing and logging tools to authorized individuals. Security events are logged, monitored, prioritized, and addressed by trained security team members. Network components, workstations, applications, and any monitoring tools are enabled to monitor user activity. Organizational responsibilities for responding to security events are defined. Critical system configuration changes create audit events, which are recorded and reviewed at the time of change. Retention schedules for the various logs are defined in our security control guidelines.

Antivirus and Malware Protection

Antivirus and malicious code protection are centrally managed and configured to retrieve the updated signatures and definitions available. Malicious code protection policies automatically apply updates to these protection mechanisms. Anti-virus tools are configured to conduct scans, virus detection, monitor real-time file write activity, and signature file updates. Laptop and remote users are covered under virus protection. Furthermore, well-documented procedures are in place to identify and eliminate unauthorized or unsupported applications.

System Backups

Anycloud has established comprehensive backup standards, guidelines, and corresponding procedures to facilitate systematic backup and restoration of data in a timely manner. Controls have been implemented to ensure the security and protection of backed-up data, both onsite and off-site. In addition, we work to ensure that data is securely transferred or transported to and from backup locations. Periodic tests are conducted to test whether data can be safely recovered from backup devices.

Network Security

Our infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats. Firewalls are utilized to help restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Anycloud maintains separate development and production environments. Our firewalls provide network segmentation through the establishment of security zones that control the flow of network traffic. These traffic flows are defined by strict firewall security policies.

Data Protection

Anycloud maintains a continuous commitment to the enhancement of our service offerings, aligning with the latest recommended secure cipher suites and protocols for encrypting data during transit. We monitor developments in the cryptographic domain and upgrade our services to respond to new cryptographic weaknesses as they are identified, implementing best practices as they evolve within the field.

Vulnerability Management

Security assessments are conducted with the primary objectives of pinpointing vulnerabilities and assessing the effectiveness of our patch management program. Each identified vulnerability undergoes an evaluation process to determine if it presents a valid risk and is assigned a priority ranking based on its potential impact. Following this ranking, vulnerabilities are assigned to the relevant team for remediation.

Patch Management

Anycloud is dedicated to the consistent application of the most recent security patches and updates across operating systems, applications, and network infrastructure to address potential vulnerabilities. Patch management processes are in place to implement security patch updates as they are released by vendors. Before deployment in the production environment, patches undergo thorough testing in a separate and controlled environment to validate the effectiveness and minimize potential disruptions.

Secure Network Connections

HTTPS encryption is configured for partner, distributor, and customer access to web applications. This helps ensure that while in transit, user data is safe, secure, and available only to intended recipients. The level of encryption is either SSL or TLS encryption and is dependent on what the web browser can support.

Access Controls

Role-Based Access

Access to information systems is provisioned using Role-Based Access Controls (RBAC). The permissions in RBAC are based on what level of access specific user categories require to perform their duties. Anycloud employees are granted a limited set of default permissions to access company resources, such as their email and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes. Processes and procedures are in place to offboard employees who are separate voluntarily or are terminated. Access to sensitive data in our databases, systems, and environments are set on a need-to-know/least privilege necessary basis.

Authentication and Authorization

We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. We enforce password best practices, such as complexity requiring both alpha and numeric characters and Multi-factor Authentication (MFA) to protect against unauthorized use of passwords. Passwords are individually salted and hashed.

Incident Management

Anycloud has a formalized Incident Response Plan (IRP) and associated procedures in case an information security incident is declared. The IRP defines the responsibilities of key personnel and specifies procedures to follow regarding any communication or notifications about the incident. The IRP is tested annually.
The security department has a dedicated Incident Response Team, with trained resources that are responsible for the various stages of our Incident Management strategy, including preparation, detection and analysis, containment, eradication, and recovery.

Business Continuity and Disaster Recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, we have implemented a disaster recovery program at all our data center locations. This program includes multiple components to minimize the risk of any single point of failure. Application data is replicated to multiple systems within the data center and, in some cases, replicated to secondary or backup datacenters that are geographically dispersed to provide adequate redundancy and high availability. High-speed connections between our datacenters help to support swift failover.

Data Protection

We apply a common set of personal data management principles to customer data that we may process, transmit, and store. We protect personal data using appropriate physical, technical, and organizational security measures. We give additional attention and care to sensitive personal data and respect local laws and customs, as applicable.
Anycloud only processes personal information in a way that is compatible with and relevant for the purpose for which it was collected or authorized in accordance with our privacy policy. We take all reasonable steps to protect information we receive from our users from loss, misuse or unauthorized access, disclosure, alteration and/or destruction. To learn more about our data protection practices read our ISAE 3000 assurance report **here.**

The NIS2 directive & Dora

The NIS2 directive and DORA play crucial roles as regulatory standards in safeguarding digital infrastructure and data integrity.

Compliance ensures that organizations implement robust cybersecurity measures, protecting against cyber threats and enhancing resilience. For companies utilizing Microsoft 365, adherence to these standards is paramount. Microsoft 365 stores vast amounts of sensitive company data including emails, documents, and collaborative content, making it a prime target for cyberattacks. Compliance with NIS2 and DORA ensures that organizations have comprehensive and compliant backup strategies in place, safeguarding critical data against loss, corruption, or unauthorized access. By prioritizing compliance, companies not only mitigate risks but boost trust with stakeholders, partners and customers, by demonstrating commitment to data security and regulatory compliance.

ACB365 IS NIS2 & DORA COMPLIANT

ENHANCES UNDERSTANDING

- ACB365's global IBM datacenters ensure compliance, reducing data breach risks for financial institutions, which aligns with NIS 2's data residency requirements.
- Our worldwide presence allows data storage in preferred regions, aligning with DORA's compliance goals.

COMPLIANCE REPORTING

- Granular visibility into user activity, data access, and backup operations facilitates compliance reporting.
- Detailed audit trails enable financial institutions to demonstrate transparency and accountability in data management, addressing DORA's requirements.

MULTI-LAYERED PROTECTION

- Segregation of duties and air gapping minimize unauthorized access risks.
- Industry-standard 256-bit encryption for data at rest and in transit safeguards sensitive financial information.
- Multi-layered data protection strategy contributes to DORA's resilience objectives.

IMMUTABLE BACKUPS

- Immutable backups protect against ransomware and insider threats, preventing unauthorized data modification or deletion.
- Unyielding backup protection ensures data integrity and availability, meeting NIS 2's data integrity requirements.

Our partnership

IBM Platinum Partner

Since 2013, our partnership with IBM has been marked by a commitment to innovation, driving the expansion of our service offerings. Our collaboration has been both intensive and fruitful, culminating in the honor of being named 'Cloud Partner of the Year' in 2017. This recognition celebrated our innovative use of cloud solutions and implementation of Watson services. IBM's role as a business partner has provided us with stability and reliability, enabling us to explore and develop new solutions. Our dedication was further acknowledged in 2019 when we received the 'IBM Technology Service Provider of the Year' award for our development of the Digital Trust model, based on IBM Trusteer. And in 2022, Anycloud proudly received the 'Business Partner of the Year for IBM Business Partner Excellence Awards' for Europe, cementing our commitment to excellence in partnership. Most recently we were awarded as with the IBM Nordic Cloud Partner of the Year 2023 and as the winner of the EMEA Partner Plus Award with the category of Modernization, which celebrates our ability to unlock new possibilities along with expanding in unexpected way, removing long-standing barriers, and enabling our distributors, partners, and clients with flexibility to build a brighter future.
Together we pioneer market leading cloud SaaS solutions that redefine the possibilities of technology by leveraging Anycloud's expertise in delivery and IBM's legacy of technology. The continuous partnership and collaboration with IBM pushed us to pursue new possibilities within technology, software, and innovation where simplicity and scalability is at the core of our operations.

DELIVER NEXT-LEVEL COMPLIANCE

- Deliver a true cloud-to-cloud backup by separating data from Microsoft environments to IBM datacenters and thereby provide segregation of duties. This brings enhanced security by avoiding dependence on a single provider.
- Bring geographical redundancy to end-customers by storing data in three local datacenters with IBM COS Regional and simultaneous storage in multiple locations providing data resilience.

Datacenter locations

AUSTRALIA
SYDNEY

BRAZIL
SAO PAOLO

CANADA
MONTREAL
TORONTO

FRANCE
PARIS

GERMANY
FRANKFURT

INDIA
CHENNAI

ITALY
MILAN

JAPAN
TOKYO

SINGAPORE

SPAIN
MADRID

UNITED KINGDOM
LONDON

USA
CALIFORNIA, SAN JOSÈ
TEXAX DALLAS
WASHINGTON D.C.

LET'S STAY CONNECTED

Anycloud A/S
Hedegaardsvej 88
2300 Copenhagen S
Denmark

CVR: DK31161509
E-mail: partner@anycloud.dk

any.cloud