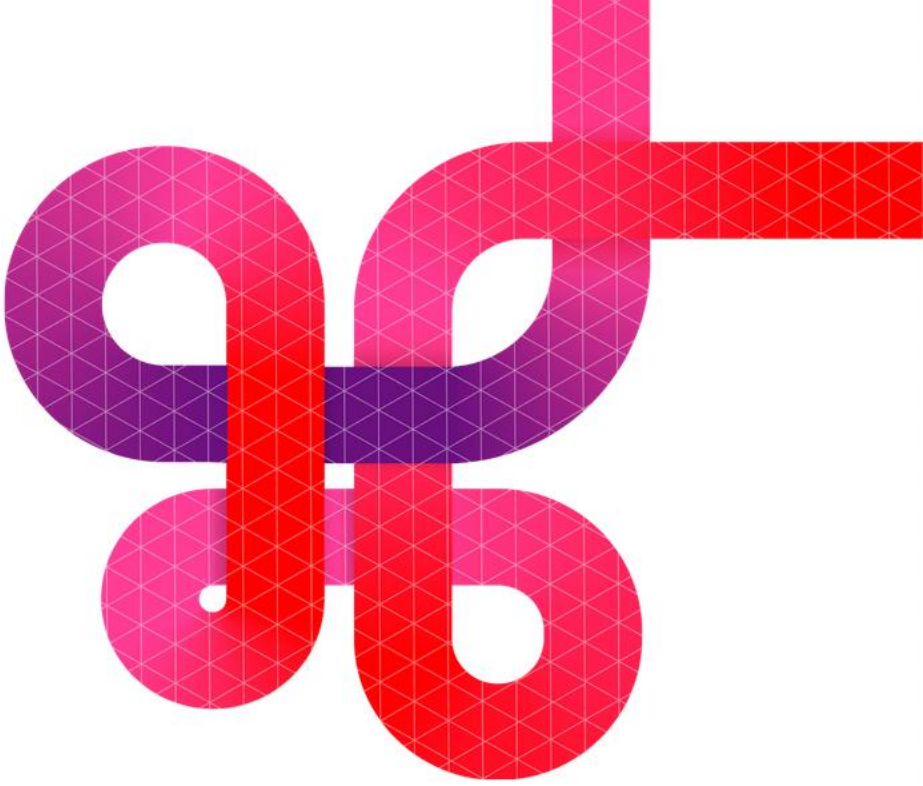


ISO 27001/ISMS

Organizational Compliance and Control

August 2019

Summary

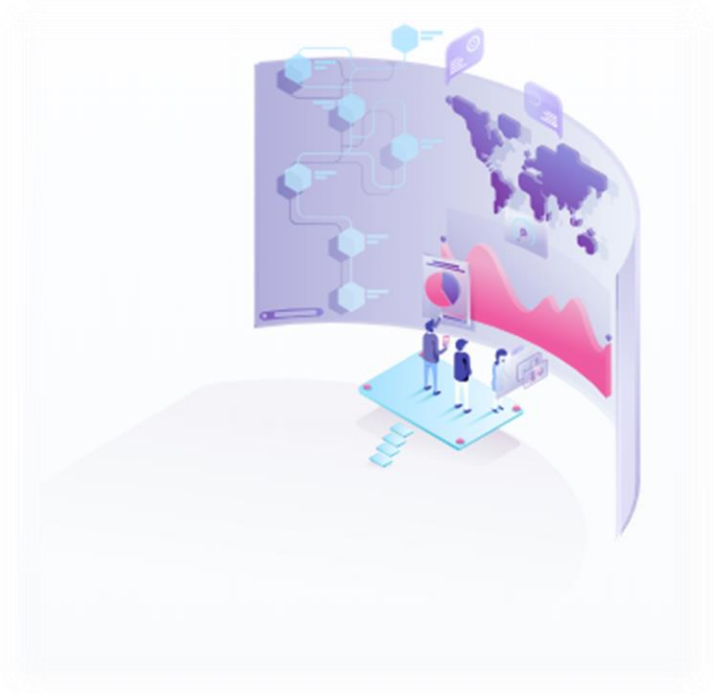
Celonis is dedicated to high security across all aspects of the organization. We are using the ISO27002 best practices as Celonis goes through the full ISO27001 certification procedures and have successfully implemented an Information Security Management System (ISMS).

Celonis is proud to provide you with our industry leading software solution that will help you tackle the challenges of the digital age, run even smoother, and grow further.

Along with developing and providing our CATEGORY DEFINING PROCESS MINING SOFTWARE - which enables you to analyze, visualize, and optimize business processes based on data and digital footprints - safeguarding processed information within our organization is one of the core responsibilities of Celonis.

Therefore, we have successfully implemented an Information Security Management System according to ISO2700o Standards to ensure the quality of our security related processes. This internal management system, its procedures, and our training measures are regularly reviewed and certified by an external auditing authority as part of our annual ISO27001 and ISO9001 audits.

The purpose, direction, principles, and basic rules of our ISO 27001 compliant Information Security Management include: conformity with internal security regulation, compliance with the protection objectives availability, integrity and confidentiality for all assets and data at Celonis.



Information Security Management at Celonis

Our security program is aligned with ISO 27000 Standards and industry best practices in order to keep all information and data safe. The focus of our security program is to prevent unauthorized access to customer data, take exhaustive steps to identify and mitigate risks, implement best practices, and constantly develop ways to improve. In order to achieve

celonis

this, we regularly review and update security policies, provide security training, perform application and network security testing, monitor compliance with security policies, and conduct internal and external risk assessments. Our approach is to combine the most accepted standards – like ISO 27001 – with compliant Celonis security measures geared to the specific needs of our customers' businesses or industries.

- **Information Security Management.** Celonis has established an Information Security Management framework describing the purpose, direction, principles, and basic rules regarding Information Security Management. This is accomplished by assessing risks and continually improving the security, confidentiality, integrity, and availability of Celonis systems. All these objectives are reviewed at least once a year. Top management determines the method of measurement, and subsequently measures the achievement of the objectives in the following domains:

- **Policies and Guidelines.** Our internal Information Security Management Team of dedicated professionals works in partnership with peers across the entire company as well as industry experts, auditors, and accredited certification authorities. Guidelines and Policies pertaining to user and Celonis information are established with regulations in key areas including device security, authentication requirements, data and systems security, user data privacy, restrictions on and guidelines for employee use of resources, handling of backups, processes of reporting potential security issues, advice on the Use of Cryptographic Controls, procedures for working in secure areas, and drafting Business Continuity Plans.

- **Certification and third-party Audits.** Our Information Security Management program is validated by an independent third-party based on ISO 27001 which is recognized as a premier information security standard around the world. Celonis, critical suppliers, and our managed service provider undergo regular third-party audits. We have established a thorough set of security policies covering the areas of physical security, incident response, logical access, physical production access, Change Management, and support, among others. These policies are reviewed and approved at least annually and are enforced by the Celonis Security Team. Our Information Security Management program was validated by an independent third-party.

• **Human Resource Security.** Upon hire, each Celonis employee is required to complete a background check and sign a security policy acknowledgement and non-disclosure agreement. Employees participate in mandatory security training when joining the company and receive ongoing security awareness education. Only individuals that have completed these procedures are granted physical and logical access to the corporate and production environments, as required by their job responsibilities. Upon termination of employment, personnel access to information systems, networks, and applications is removed and the personnel returns all company provided devices.

• **Physical Security.** There are extensive regulations and measures on how we maintain a safe and secure environment for people and property at Celonis. The Celonis Physical Security Team is responsible for enforcing our physical security policy and overseeing the security of our offices. Physical access to subservice organization facilities where production systems reside are restricted to personnel authorized by Celonis, only as required to perform their job function.

• **Dedicated Security Zones.** Any individuals requiring additional access to production environment facilities are granted that access through explicit approval by appropriate management. A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals. Access to areas containing corporate servers such as server rooms is restricted to authorized personnel only. The lists of authorized individuals approved for physical access to corporate and production environments are reviewed on a regular basis in compliance with Information Security Standards.

• **Visitor Management and Access Control.** Physical access to corporate facilities is restricted to authorized Celonis personnel. A badge access system ensures only authorized individuals have corporate facilities access. Visitors are accompanied and do not have access to critical information and facilities. Access areas to information processing facilities are monitored, recorded, and controlled at all hours.

• **Access Control and Logging.** We have established extensive policies and measures for securing Celonis systems, user information, and Celonis confidential company information. These policies cover access control to corporate and production environments as part of our Information Management System. Our internal policies require that employees accessing production and corporate environments adhere to best practices for the creation and storage of SSH private keys. Celonis employs technical

access controls and internal policies to prohibit employees from arbitrarily accessing user files and to restrict access to metadata and other information about users' accounts.

• **Physical Production Access.** Our procedures include safeguards for restricting access to the physical production network, including management review of personnel and de-authorization of terminated personnel. Access to resources including data centres, server configuration utilities, production servers, and source code development utilities is granted through explicit approval by the appropriate management staff. A record of the access request, justification, and approval are recorded, and access is granted by appropriate individuals only. We also have our systems operating in separate networks to better protect sensitive data. With systems supporting testing and development activities hosted in a separate environment from systems supporting our production infrastructure, we ensure secure continuous development and operations.

• **Change Management.** In order to maintain a robust and secure operational performance and provide our excellent software solutions to our customers without any interruptions, policies and practices are in place that steer code reviews and manage changes by authorized developers that may impact the security of application source code, system configuration, and production releases.

• **Information Backup.** Information systems, computers, and software involved in the performance of the services provided are backed up regularly. Backups are tested in accordance with operational backup standards. Information that is stored on backup media is protected against unauthorized access, misuse, or corruption at all times.

• **Security Testing and Incident Handling.** In addition to our compliance audits and internal tests, we engage independent entities to conduct penetration tests. Results of these tests are shared with senior management and are triaged, prioritized, and remediated in a timely manner. Our requirements for incident reporting and breach notification cover responding to potential security incidents, including assessment, communication, and investigation procedures. Reported security incidents are classified, prioritized, and logged. Our Suppliers are also contractually bound to promptly notify Celonis in the event of an information security incident and report any potential impact on the Supplier's capability to perform services for Celonis.

• **Business Continuity and Disaster Recovery.** At Celonis, we have established a Disaster Recovery (DR) program and maintain a documented organizational Business Continuity

Plan (BCP) which are designed to ensure that we will continue to function through operational interruption and will be able to provide services to all our customers as specified in our agreements.

• **Supplier Security.** To run efficiently, Celonis relies on sub-service organizations. All sub-service organizations undergo a screening process as part of our partner onboarding. We choose best of class industry partners to provide our category leading solution and professional services. We take appropriate steps to ensure our security standards are maintained by establishing agreements that require sub-service organizations to adhere to confidentiality commitments we have made to users. As part of that, we monitor the effective operation of our subcontractors´ safeguards. We review of all our subcontracted service organizations' controls and adherence to ISO 27001 security standards regularly performed by either third-party credentialed assessors or suppliers' internal risk and compliance team.

Disclaimer

This document is provided for informational purposes only. It represents Celonis' current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Celonis' products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances. The responsibilities and liabilities of Celonis to its customers are controlled by Celonis agreements, and this document is not part of, nor does it modify, any agreement between Celonis and its customers.