01.CP_06 - Information Security Policy Document (ISPD)

Version 25/07/2024

Introduction

The purpose of this policy is to define the strategic directions adopted by Arcchiva Group (hereinafter also just "Archiva") to safeguard the security of information, people,companies, organizations and nationsthat interact to any extentwith Archiva S.r.l. a socio unico , information security risks and cyber risks.
This policy informsall stakeholders, internaland external, on the guidingprinciples relevant for the entire data viewing cycle pursuant to Regulation (EU) 2016/679 and pursuant to Regulation (EU) 2018/1807.

Archiva considersthe protection of information assetsa primary aspectfor the protection and continuity of its business and the business of its customers.

Archiva aims to ensure that:

- the information is protected from unauthorized accessor improper use;
- the confidentiality of the information is guaranteed;
- the integrity of the information is maintained;
- the cybersecurity concepts (identify, protect,detect, respond and recover) are understood, implemented and constantly monitored and updated;
- the availability of information and information systemsis maintained for the provisionof services;
- business continuity planning and implementation processes are maintained;
- regulatory, contractual and legal requirements are respected;
- physical, logical,environmental and communications security is maintained.

This policy was approvedby Archiva's Management and represents the company's commitment to Information Security, Cybersecurity as well as integrating its business continuity objectives. The same is subject to annual review and updating in the event that significant changes have occurred, in order to always guarantee its suitability, adequacy and effectiveness.

Terms and definitions

For the purposes of this document, the terms and definitions given in:

- ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary;
- Regulation (EU) 2016/679;
- Regulation (EU) 2018/1807;
- Guidelines on the formation, management and conservation of electronic documents. (AgID).

Scope of the document

This document aims to define the information security policy of Archiva, in its role as Conservator, as well as FinancialIntermediary towards the SDI and Data Controller, Data Processor (or other manager) pursuant to art. 28 Regulation (EU) 2016/679.

Archiva has implemented an Integrated Management System (IMS), including an Information Security Management System according to the technical standard ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements), having as its scope of certification the "Design, development and maintenance and provision of services and software products in SaaS mode, electronic invoicing, conservation of electronic documents, through electronic signature techniques, dematerialization of paper archives through the application of the ISO Guidelines /IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701. Electronic signature solutions"

Nota 1: ISO/IEC 27017 (Information technology - Security techniques - Code of practice for information securitycontrols based on ISO/IOEC27002 for cloud services);

Nota 2: ISO/IEC 27018 (Information technology - Security techniques - Code of practices for protection of personally identifiable information (PII) in public cloud acting as PII processors);

Nota 3: ISO/IEC 27701 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC27002 for privacy information management — Requirements and guidelines.

This document is also effective for what is required by the ENX consortium regarding TISAX certification.

Archiva pursues the continuous improvement of its Information Security Management System on a daily basis by providing a fundamental support service to the company's "core business" through tools and means technologically in line with progress and maintaining them in a perfect state of efficiency. The Company defines the roles and responsibilities of the personnel involved in the management of information security. Periodically and systematically identifies threats that can cause damage to data, assessing their exposure to risks and implementing appropriate mitigation actions.

Archiva constantly trains staff involved in any processing of personal data, in order to protect company assets in compliance with applicable law. It also implements awareness programmes, aimed at employees, external consultants, partners and other subjects possibly involved in any type of processing, on information security and data protection, with particular attention to confidentiality, integrity and to the availability of the information and the personal data processed.

Objectives

Archive by defining the company guidelines regarding data protection, on the basis of their classification in terms of Confidentiality, Integrity, Availability, identifies the following objectives:

- strategic objectives:
  - pursue and maintainregulatory compliance regarding information security. Archiva S.r.l. a socio unico pursuescompliance with the laws and regulations applicable in every operating context and respects the technical standards relevant to the organisation's activity.

- tactical objectives:
  - o definegeneral guidelines applicable in all corporatecontexts, to information security, quality, Data Protection and Privacy;

- operational objectives:
  - start the drafting, publication and periodic review of procedures and operational instructions necessary for the achievement of more general tactical and strategic objectives.Archiva definendo le linee di indirizzo aziendaleriguardanti la protezione dei dati, sulla base della loro classificazione in termini di Riservatezza, Integrità, Disponibilità individua i seguenti obiettivi:

The following documents describing the objectives were also definedand shared with stakeholders:
- Information security objectives
- Objectives for business continuity
- Quality objectives
- Objectives for the prevention of corruption
- Objectives for environmental management

This document is made available to the entire company, through the information systems adopted, and kept periodically updated on the basis of the necessaryregulatory and technological adjustments that become necessary from time to time. Sono stati inoltre definiti e condivisi con gli stakeholder i seguenti documenti di descrizione degli obiettivi:

Guiding principles

This document is made available to the entire company, through the adopted information systems, and kept periodically updated based on the necessary regulatory and technological adjustments that become necessary from time to time.

The following goal description documents have also been defined and shared with stakeholders:

- staff training is an essential element to prevent the occurrence of unwanted adverse situations whichmay result in damage to the companyand the stakeholders involved;
- specific training in the design of services,processes and applications is an indispensable element to guarantee the implementation of solutions that can correspond to the real needs of the customer, in compliance with the most accredited guidelines and reference practices.
- continuous monitoring of threats and vulnerabilities is essential to guarantee the security and effectiveness of the systems and services provided to customers;
- the continuous evaluation of the security measures adopted is essential to guarantee that all stakeholders maintain the minimum information security requirements. Archiva S.r.l. a socio unico attaches primary importance to the security of information, whether worked on behalf of its clients or handled in person, in view of the growing trends of threats and vulnerabilities, the difficulty of maintaining effective security measures over time, and in fine the corporate culture and sensitivity of the personnel involved in business operations.

Roles and responsibilities

The matrixbelow shows the roles and responsibilities assignedto each phaseof the life cycle of this document.

Activity	Responsible	Executor	Consulted	Informed
Editig, publication	Company Management	CISO,CTO	Department Manager, DPO	HR
Adoption	Department Manager	Stakeholder internal e external		
Review	Company Management	CISO	Department Manager, DPO	HR

Company Management

The Company Management has overall responsibility for the definition of the generalprinciples that regulate the security of Information and their effective translation into internal operating procedures, necessary to satisfy and guarantee the correct functioning of the operational processes themselves as well as compliance with the reference regulatory framework and the agreed contractual requirements.

CISO

Il Chief Information Security Officer is responsible for maintaining this document. The drafting of specific further policies, procedures and operating instructions is entrusted to the individual company functions involved from time to time.

The Chief Information SecurityOfficer (CISO) reportsto the Management of ArchivaS.r.l. a socio unico and has the following responsibilities:

- define and update the Information Security policy basedon Archiva Securityguidelines;
- design the protection systemand prepare plans for its implementation;
- coordinate the implementation of the protection system;
- monitor the implementation of protection systemsand protection measureson the assets of information systems;
- promote training, awareness and communication initiatives and programs on IT security;
- promote audit and evaluation activities for the continuous monitoring of the adequacyand effectiveness of the information protection system;
- report the status of the information security system, plans,actions and problemsto the Archiva Management.

The CISO is also responsible for the IMS and, therefore, is responsible for:

- design the IMS and prepare plans for its implementation;
- coordinate the implementation of the IMS;
- maintain and monitor the IMS is responsible for the maintenance of this document. The drafting of specific additional policies, procedures and operating instructions is left to the individual business functions involved from time to time.

CTO

The Chief Technology Officer (CTO) reports to the Management of Archiva S.r.l a socio unico and has the following main responsibilities:

- define the objectives and strategies for the IT department;
- select and implement the right technology to streamline all internal operations and help optimize their strategic advantages;
- design and customize technological systems and platformsto improve the Customer Experience.

The CTO is also the Head of the IMS and, therefore, is responsible for:

- plan the implementation of new systemsand provide guidanceto IT professionals and other personnel within the organization;
- approve purchases of technological equipmentand software and establish partnerships with IT suppliers;
- supervise the technological infrastructure in the organization (networks and IT systems), to ensure optimal performance;
- manage and organize projectsrelated to the IT field;
- monitor technological changes or advancesto discover ways in whichthe company can gain a competitive advantage.
- Analyze the costs, value and risksof information systemstechnology to advisemanagement and suggest actions.

DPO

The DPO (Data Protection Officer) within the scope of this document has the task of informing and providing advice to the Data Controller or Data Processor as well as to the employees who carry out the processing activities about the obligations arising from this document, by the Regulation as well as by other provisions of the Union or Member States relating to data protection. The DPO also has the task of supervising compliance with this documentwith regard to the processing of personal data and acting as a contact point for the supervisory authority for issues related to the processing.

Department Manager

The Department Managers of Archiva S.r.l a socio unico are required, according to their responsibilities, to apply and monitor the implementation of all the rules regarding information security and to report to the Company Management, the CTO and the CISO any question on the security status of the information (e.g.: system violations, progress of compliance with security measures,etc.). They are also required to inform suppliers and consultants who carry out activities on behalf of Archiva of the guidelines and protection procedures necessary for the processing of information.

Managers must work to ensure the translation of the principles defined through this policy within their departments and the processes governed by them.

Internal users

Internal users (employees/collaborators) process information based on instructions and authorizations defined based on specific operational profiles. Internal users are responsible for adopting behavioral measures in line with the principles defined in this policy document and with the Operating Instructions for those authorized to process data drawn up pursuant to art. 29 of Regulation (EU) 2016/679. Internal users are also required to know and respect the Company Regulations and the Company IT Regulations. Any behavior in violation of the above will be evaluated from time to time by the CompanyManagement, which from now on reserves the right to resort to disciplinary actions as already provided for by the relevant CCNL.

EVERY EMPLOYEE AND COLLABORATOR OF THE ARCHIVE, AS WELL AS EXTERNAL USERS WHOM FOR SPECIFICREASONS IS GRANTEDACCESS TO THE COMPANY INFORMATION SYSTEMS, IS REQUIREDTO COMPLY WITH THE PROVISIONS OF THIS INFORMATION SECURITY POLICY.

VIOLATION OF THIS POLICY AND OF THE SECURITY REQUIREMENTS DESCENDING FROM IT, MAY RESULTIN DAMAGE TO THE COMPANYWHICH HEREBY RESERVES THE RIGHT TO TAKE DISCIPLINARY MEASURES OR LEGAL ACTION IN THE APPROPRIATE FORCES.

Main expected results

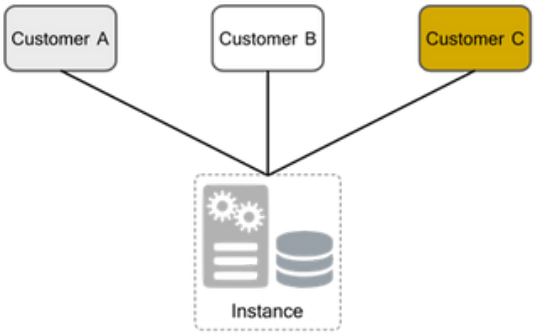
The introduction of this policy lays the foundation for the definition of further policies, procedures and operational instructions which are now inspired and informed by the general principles defined here, with the application of which the Company wants to guarantee the achievement of the strategic objectives above cited.

Relationships with other policies

Any other further policy implemented by Archiva is implicitly linked to this policy.

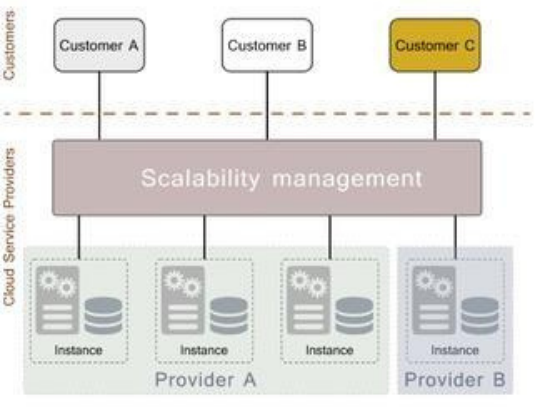
Specific considerations for the provisionof cloud services and for the processing of personal data in the cloud

Starting from 2019, Archiva has started a process of approaching the provision of services rendered to customers via the cloud. Archivahas now adopteda "Multi-tenant SaaS application" model, schematized in the following illustration: (image taken from AgID circular no. 3 of 9 April 2018).



A single application instance simultaneously serves multiple customers, who access the same application instance runningon shared virtualresources. The isolationof data and users occursat the application, database management (DBMS) and storage levels, using the appropriate authentication, authorization and security mechanisms.

In the process of renewing your infrastructure, orientedtowards the Cloud,the new model, illustrated below, will allow you to have more flexible configurations.



Customers will be able to have their application instance running on shared or dedicated resources (or a mix of the two) in a transparent and configurable manner. The load balancing system allows you to implement allocation policies (of new application instances) based on a multitude of criteria (one of the most important is the quality of service). Application instances can be added and removed dynamically at any time and based on needs. The virtual resources needed by applications are also dynamically allocated. The allocation of new application instances or virtual resources does not require any architectural modification of the system that has alreadybeen created in order to adapt dynamically. All this allowsus to offer and implement diversified SLAs for the various customers.

The Archiva security baseline, thereforeextends to the security controlsof the above-mentioned guidelines, which must, therefore, be taken into consideration for what is declared in the certification scope,with particular referenceto the design and development of products aimedat creating services that will be provided via the cloud.

This new perspective also requires that:

- the logical and, where relevant, physical segregation of the application environments granted for use to customers is verified;
- the possibility of accessing customerinformation (assets), hosted and processedin the cloud, is always verified;
- the communication procedurewith customers is periodically verifiedand updated when changes are applied;
- the security of the virtualized environments on whichthe cloud infrastructure is based is periodically verified;
- a process of revaluation of the utilitiesgranted for use to customers is periodically carried out;
- communication of Data Breaches and support for related investigative activities is envisaged.

All services provided in the cloud are under the control of the "Archiva Information Security" structure (see HLP_02 Leadership). At the end of the service design phase, the Project Management function communicates the customer's references to the CustomerCare function for subsequent and any assistance activities.

Archiva undertakes to observe, amongothers, the legislation in force from time to time regarding Data Protection & Privacy.

Cryptographic Controls

In consideration of its activities as an intermediary towards the SDI and as a Conservator, registered in the AgID Conservatori Marketplace, from which the consequent general, quality, security and organizational constraints derive, Archiva in orderto protect the data processed on behalf of its Customers when these are at rest,it can adopt cryptographic mechanisms, based on what was agreed when drafting the project. Archiva has equipped itself with an internal procedure "POA.SYS.07 - Use of cryptography", containing further general elements of the aforementioned cryptographic mechanisms to protect data in transit.

Change Management

All major changes made to the services provided to customers must be communicated in advance, indicating the date of application of such changes,their description and any impactson customer operations. Archiva has implemented a change management process, governed by the internal procedure “POA.CISO.05 - Change management”.

Backup

Archiva implements various specific backupsolutions for the data processedand for the virtual server environments used in the provision of application services.

Archiva implements 2 different backupsystems:

- Veeam Backup & Replicator for Databases, Servers and application servers;
- SnapMirror and Snapvault for documents, also supported by Snapshot Copy.

The backup copies are positioned inside the server farm at the registered and operational headquarters of Archiva S.r.l. a socio unico in Villafranca di Verona, and replicated within its own AWS Cloud environment, located in the "Milan" region, with further replications, for business continuity aspects, at the technological centers of Cornaredo (MI), Ponte San Pietro (BG). Archiva has implemented a backup management process, governed by the internalprocedure "POA.SYS.13 Backup/restore management procedure".

Logging e monitoring

Archiva keeps logs of the various components that contribute to the definition of its infrastructure, including both network equipment and software elements. Archiva has also implemented a proactivealerting system that notifies an internal distribution list of any relevant circumstances. The monitoring systems and consequently the connected alerting systems are divided into:

- monitoring of infrastructural measures, where the object of the measurement are machine parameters and which therefore allow measurements carried out on hardware systems such as Storage, ServerProcesses, Network Equipment, Connectivity, Windows Processes and Java Demons;
- functional application monitoring, where the object of the measurement is the execution of functional processes such as for example the request to view a document, the storage of a payment package, the transformation of data, the authentication login to a web application.

Further detailson the structuring of the logging and monitoring systemadopted by Archiva are contained in the POA 26 Log and Monitoring of the SdC.

Clock Syncronization

All serversused by Archiva S.r.l. a socio unico they use the time reference offeredby the I.N.RI.M (National Metrology Research Institute) via NTP protocol to synchronize their clocks.

Archiva customers can synchronize theirinformation systems, using the same NTP servers, listed on the website https://www.inrim.it/node/643.

Management of technical vulnerabilities

In order to monitorthe technical vulnerabilities that may arise during the provision of application services to customers, Archiva has adopted a process inspired by the ISO 30111:2019 - Information technology — Security techniques — Vulnerability handling processes standard.
Over the course of a calendar year, Archiva plans at least 4 separate Vulnerability Assessment sessions on the external perimeter, exposed on the internet, and scans on the internal perimeter. Any critical vulnerabilities are immediately analyzedand their remediation is planned within 15 days.

Security measures

Archiva, in carrying out its activities as Data Controller, adopts the controls indicated in Annex A of ISO/IEC 27001 as a securitybase line. These controls, also extended to the ISO/IEC27017, ISO/IEC 27018 guidelines and ISO/IEC 27701,are evaluated annuallyduring internal auditsand third-party audits.

Security Operation Center - SOC

In order to guarantee adequate security levelson a permanent basis, Archiva has implemented a SOC with the collaboration of a specialized external supplier who monitors the company's web exposure 24/7, also investigating the deep and dark web, in order to to reveal any traces of malicious activity on the darkweb and deepweb.

Network Operation Center - NOC

In order to guarantee adequatesecurity levels on a permanent basis, Archiva has implemented an NOC with the collaboration of a specialized external supplier who monitors the entire ArchivaIT infrastructure 24/7, in order to reveal traces of any system anomalies.

Responsibilities and procedures

If, when using the application services, the customerencounters anomalies or detects events that may have repercussions on the security of the information processed by Archiva or directly

information security incidents, he can report any circumstance and/or event by writing to the email address security@pec.archivagroup.it or, alternatively, ciso@archivagroup.it. Any request for assistance relating to the use of the services provided by Archiva can be forwarded via the ticketing portal https://archivagroup.atlassian.net/servicedesk/ or by writing to the email address ticket.care@archivagroup.it.

All reports opened via the portal are tracked within the Archiva systems with a specific ticket. All reports of information securityevents are trackedin a specific register. For events classified as an information security incident or data breach, an incident report is available.

Collection of evidence

Archiva maintains within its information systems evidence of the correct implementation of the integrated management system to support certification activities. Archiva ensures maximum collaboration with customers to allow them to respond to any verification and inspection activities, requested personally or by supervisory authorities, while protecting the confidentiality of particular technological, implementation and procedural aspects specific to Archiva.

Risk management

Archiva Srl has defined a systematic approachto risk management in order to identify, analyze, evaluate and manage risks related to the Confidentiality, Integrity and Availability of protected information.

The CISO figure is responsible for leading the periodic risk management process.

Report

The CISO presents Archiva Srl a socio unico with an annualreport on the adequacy of the protection system and the progressof the implementation plans. It also reportsthe results of information security audits.

Audit

Periodic audit activities on security, information security and the Integrated Management System are planned and carried out in order to:

review the adequacy of controls and the effectiveness of the integrated management system, identifying possible improvements;
verify the adequate implementation of policies and rules, identifying possible critical situations;
report relevantinformation security mattersto the CEO;
verify the effectiveness of information protection systems through the assessment of vulnerabilities on systems and networks.

Information securityaudit activities are coordinated by the CISO.

ISO/IEC 27018 & ISO/IEC29100 - Data Protection Principles

1 - Consent and choice

Archiva, as Data Processor, as defined in the deed of designation signed with the customers, undertakes to support the Data Controller in compliance with all its regulatory constraints.

2 - Purpose legitimacy and specification

The data processing carriedout by Archiva takes placefor the sole purposes and according to the methods agreed with the Data Controller in the act of designation as Data Processor.

3 - Collection limitation

Archiva, in the role of Data Controller, does not have the right to chooseall the personal data to be processed, since these are provided directly by the Data Controller (Customer).

4 - Data minimization

Archiva undertakes to use only the data strictly necessary for the declared purposes and to eliminate from its information systemsany temporary files or workingdocuments no longer necessary for the processing of the Data Controller's data.

5 - Use, retention and disclosure limitation

Archiva providesthe possibility of giving accessto the Data Controller's data,at the request of the competent supervisory authorities, without delaying access and by promptly informing the Data Controller, as provided for in the act of designation as Data Controller. This diffusion is kept track of in specific documentation.

6 - Openness, transparency and notice

Archiva makes known any use of additional data controllers (as identified in Article 28, paragraph 4 of EU Regulation 2016/679), communicating their involvement in the act of designation as Data Controller.

7 - Accountability

Archiva, as Data Processor, undertakes to notify the Data Controller of any violations of his personal data, accordingto the methods and timescales defined in the Data Processor designation agreement. In the event of a Data Breach,Archiva draws up a specificreport whose structure corresponds to what is indicated in the art. 33 of Regulation (EU) 2016/679.

In order to support any forensic investigations over time, Archiva maintains within its information systems an updated and historicized copy of all the policies, procedures and operational instructions necessaryfor the operation of the Integrated Management System.

If the Data Controller requests the returnof their information assets (the documentsstored within the CS), Archiva will apply the provisions of the POA 01 procedure - Management of Waste from the Conservation System.

8 - Information security

- all employeesand any collaborators of Archiva are subject to specific confidentiality agreements;
- in order to prevent unauthorized copying of information on mobile or transportable devices, Archiva adopts DLP mechanisms, which promptly report any attemptsat unauthorized copying;
- all data restore activities are tracked in specific application logs;
- the data transmitted by the Data Controller are not stored on mobile or removable devices, except in caseswhere the Data Controller requestsa copy of such data on opticalmedia. In these circumstances, the data is stored in compressed directories protected with strong passwords, communicated to the Data Controller with communication channels different from the one used for data transmission;
- all data in transitbetween the Ownerand Archive are exchanged throughencrypted communication channels (SSL/TLS1.2);
- the destruction of the analogueoriginals or theircopies, transmitted by the Data Controllers, takes place by means of a contracted sub-supplier, who performsthe certified "paper pulping" service;
- each user who accessesthe Archiva information systems, through which business servicesare provided to the Data Controllers, uses unique, non-generic, non-technical authentication credentials;
- the list of users authorized to access the Conservation Systemis periodically reviewed;
- expired and/ordeactivated users are not reassigned to other users;
- the act of designation as Data Controller indicates the minimumsecurity measures implemented by Archiva in the provision of its services;
- the technical organizational measures agreed between the Data Controller and Archiva are extended, where relevant, to any additional managers involved in the processing;
- any reuse of mass storage devicesoccurs only following deep deletion of the support'sfile system;
- Archiva processes the personal data of the Data Controllers exclusively within the national territory, at the headquarters in Villafranca di Verona (VR).