CODE OF ETHICS

Archiva S.r.l
Date: 09/2021
Version: 01
Code: COD_ET_01

Revision Matrix

Version	Date	Description	Approval
00	17/04/2015	Issue	Giuliano Marone Chairman of the Board of Directors
01	20/04/2016	Review	Giuliano Marone Chairman of the Board of Directors

Index

1 INTRODuCTION

Archiva S.r.l., a company specialising in the outsourcing of business processes focused on business documents, offers a range of "cloud" services, dedicated to the issuance, control, consultation and substitute storage of all flows, both active and passive, in line with the new Technical Rules on the storage of IT documents.

By freeing information from its physical dimension and making its pure content usable anytime and anywhere in a fast and secure manner, it proposes itself as a strategic partner of its client companies.

Archiva S.r.l. is today one of the main players in the document archiving and regulation-compliant preservation market, with more than 40 million certified documents and more than 83 million images processed per year, more than 380 million documents published online and more than 200,000 documents consulted daily on the web, and 100 collaborators and professionals serving over 500 companies.

The **"Mission"** is to be a strategic partner for the management of contents related to business documents. Our commitment, aimed at simplifying the flow of information in compliance with the regulations, is the added value for our customers in order to free the information from its physical dimension through the immediate achievement of pure content.

The **vision of** Archiva S.r.l. is that of a future in which complete, fast, secure, and available information will be among the first critical success factors in business processes.

Due to the size and importance of its activities, Archiva S.r.l. is an industrial group aware to play a relevant role with respect to the market, to the economic development and to the welfare of the people working or collaborating with Archiva S.r.l. and of the communities where it works.

The reliability and reputation of Archiva S.r.l. are factors that constitute a decisive asset for the success of the company and for the improvement of the social context in which it operates.

The established principles aim at imprinting fairness, equity, integrity, loyalty and professional rigour on the operations, behaviours and working methods of all legitimate stakeholders in the company's business, both in internal and external relations.

Clarification: in this document, the company name Archiva S.r.l. may hereafter be abbreviated to Archiva.

2 General principles - corporate values and ethical principles

The present document "Code of Ethics" contains a set of values, principles and rules whose observance by the recipients is of fundamental importance for the proper functioning, reliability and reputation of Archiva S.r.l.. The recipients of the code include the Directors, Auditors, Management and Employees of ARCHIVA as well as all those who work to achieve the objectives of ARCHIVA.

The Code of Ethics also constitutes the first safeguard on which the Organisational, Management and Control Model adopted by the Company is based, in accordance with the provisions of Legislative Decree 231/01 (Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law 300 of 29 September 2000), of which it is an integral part.

Violation of the principles and rules contained therein may therefore lead to serious consequences for the Company, also under the said legislation.

ARCHIVA is committed to promoting awareness of the Code of Ethics among ARCHIVA staff and other Stakeholders and their constructive contribution to its principles and contents.

ARCHIVA will in any case carefully monitor compliance with the Code, setting up appropriate information, prevention and control tools and procedures and ensuring the transparency of the operations and behaviour carried out, taking corrective action if necessary.

The Supervisory Board of ARCHIVA is assigned the functions of guarantor of the Code of Ethics.

The Code is brought to the attention of all those with whom ARCHIVA has relations.

2.1 Innovation and protection of intellectual property

The attention to new technologies and the continuous search for optimisation of the production processes are inspiring principles of ARCHIVA's activity.

ARCHIVA promotes research and innovation activities by Management and Employees, within the scope of their functions and responsibilities. The intellectual assets generated by this innovative activity are a central and indispensable asset of ARCHIVA.

Research and innovation are dedicated to the promotion of products, tools, processes and behaviours that are increasingly favourable to energy efficiency, the reduction of environmental impact, attention to the health and safety of employees, customers and in general to the sustainability of business activities.

ARCHIVA's People are expected to contribute actively, within the scope of their functions and responsibilities, to the governance of intellectual property to enable its development, protection and enhancement.

2.2 Technological solutions for IT security

The focus on new technologies and the continuous search for state-of-the-art security solutions are inspiring principles of ARCHIVA's activity.

2.2.1 Perimeter Network: Service Availability - Geographical Load Balancers

ARCHIVA provides its services through the Internet, so the availability of Internet access is of paramount importance for the company's business and to ensure that its customers can access their archived documents without interruption.

For this purpose, Archiva has equipped itself with a couple of geographical load balancers, able to expose its web services on two internet accesses of different providers that are connected to different POP (Point of Presence). If one of the two Internet accesses is not working, the system automatically inhibits the publication of the service on the link of the provider that is having problems, leaving only the link still active to manage all the traffic towards the Archiva network.

In a normal situation Clients use both links, being directed alternately to one and the other to balance the workload.

2.2.2 Perimeter Security: Intrusion Prevention System

Archiva has implemented a market-leading network traffic inspection system. This system aims to analyse all network traffic, both incoming and outgoing, for anomalous behaviour that may indicate virus, malware or hacking activity.

The implemented system, which is at the top of the IPS performance and functionality, allows to analyse the behaviour of the web or ftp session. If anomalies are found, the system automatically

blocks the session and the suspect source IP address, preventing it from reaching Archiva server or client systems.

This solution also makes it possible to preemptively block all traffic from countries with which we do not have a business relationship (e.g. New Zealand, African countries or Oceania), from which targeted attacks on companies/institutions/associations are known to originate. Archiva has decided to maintain the possibility of unrestricted access only from countries in the European Union, the United States of America and Canada, and from public IP addresses of its customers' offices in Russia, Asia and Latin America.

The IPS system detects malware, worms, viruses, botnets (computer networks dedicated to spreading computer threats), spam and public IP addresses known to be dangerous by comparing various parameters with a proprietary database that is updated several times a day following the discovery of threats; Archiva updates this database on its own equipment on a daily basis in order to always be in line with the latest known threats. The system integrates a device for storing logs for event analysis.

2.2.3 Perimeter Security: Firewall

Once the coherence of the network traffic has been verified through the IPS system, the next line of defence is represented by the pair of highly reliable stateful firewalls, which, based on ACL (Access Control List) verify that the service that the external client is trying to access is actually among those that Archiva decides to make available, typically HTTP, HTTPS, FTP and SFTP web services. This means that an external user will only be able to access services published on TCP port 80 or TCP port 443, if they try to access TCP port 445 they will be denied access.

All firewall logs are stored in real time on a log archiving system that allows analysis of what is happening at the level of block events and at the level of network traffic.

These firewalling systems, as well as all other infrastructural security components, are fully managed by Archiva's highly qualified in-house staff, who monitor their configuration consistency and periodically check their security status.

2.2.4 Perimeter security: Reverse Proxy - Load balancer

Downstream of the firewall pair is the DMZ (Demilitarised Zone), a particular portion of the Archiva network that contains the equipment most exposed to access by customers, and which is therefore in a network with special security features.

Archiva decided not to expose any server directly to the Internet, to reduce the risk of running into security bugs in operating systems or applications, but to publish "dummy" servers represented by the Reverse Proxy that simulates a service in all its parts, not allowing direct access to the final server by the user. This technique makes it possible to exclude the security problems associated, for instance, with Windows Server 2008 or IIS services, since the Reverse Proxy does not carry such insecurity elements. A possible attacker cannot exploit the vulnerabilities of Linux, Windows, Intenet Information Services, Jboss, Apache or Websphere because he cannot reach

them, he can only reach the Reverse Proxy which, by definition and characteristics, is a machine without vulnerable systems.

2.2.5 Perimeter Security: Antispam Systems and Mail Relays

Within the Archiva DMZ network is hosted the pair of Antispam systems, devices responsible for receiving all email flows from the Internet (Mail Relay) and analysing the content of individual email messages (Antispam). The pair provides high reliability, ensuring that the failure of one of the two appliances does not compromise the availability of the email reception and dispatch service.

The introduction of the IPS system has given Antispam systems a considerable advantage, since all the flow to be analysed that reaches them has already been assessed by the IPS (looking for spammers or senders known to be compromised), so that what is forwarded to Archiva mail systems undergoes two merit checks, guaranteeing an excellent level of security and accuracy.

2.2.6 Perimeter Security: Web Filtering - Internet browsing control

Just as it is considered important to verify the network traffic to the Archiva network, it is equally important to evaluate and control the network traffic generated by the Archiva network to the Internet; the security solution implemented includes a Web Content Gateway, a world leader in security systems for controlling web browsing.

This system allows, while maintaining the user's security and privacy criteria, to verify in real time which site or URL the internal Archiva user is trying to access. This information is compared with a proprietary database of the solution, which is fed 24 hours a day, and which identifies sites containing threats, and even if they do not contain threats they are categorised according to the content they display. Archiva has defined, and communicated, well-defined policies that allow access to different categories of sites, other categories can be consulted for a finite number of times per day, while the categories considered dangerous, distasteful or in any case not appropriate for work are blocked in advance.

These actions prevent access to sites that could infiltrate threats, even unknowingly, into the Archiva LAN.

2.2.7 Internal Network - Internal Security: LDAP policies

Each Archiva user with a PC workstation has a personal username and password to access the internal network.

System administrator users are provided with special users that they use only when they need to perform specific tasks; during normal work sessions, administrator users use their standard user account, which has similar, and therefore limited, privileges to those of all other Archiva domain users.

All client workstations are subject to specific LDAP policies, which restrict access to the main PC settings to administrators only, and which activate the screen saver with password unlock after 10 minutes of inactivity.

Each Client resource or document is located on specific network shares, or Shares, exposed by an Enterprise NAS; each share has been configured with ad-hoc permissions that may allow the content to be read, modified or completely prevent access.

Each user only has access to the portion of the data necessary to do his job, any other action being precluded by the LDAP authentication system and the ACLs on the shares. The so-called Least Privilege Access policy is adopted to limit authorisation to what is strictly necessary.

For each shared folder, there are two groups, one with the right to read and one with the right to edit, with each user being able to belong to either one or the other, so that it is clear for each account what rights it has over individual shares.

2.2.8 Internal Security: Data Loss Prevention System

All client workstations are equipped with a software agent, centrally controlled by a server system, which checks and controls the actions performed on the network resources containing the clients' documents; this system is able to understand what actions are being performed on the image document, for example inserting it as an attachment in an email or copying it onto a USB key, blocking these actions in advance in order to minimise the risk of accidental or voluntary loss/diffusion of the data.

To date, the system implemented allows the following actions taken on customer documents to be blocked:

- Copy to USB drive
- Copy to local PC disk
- Printing the document
- Attaching the document to an outgoing e-mail
- Uploading the document to cloud services such as DropBox or iCloud
- Uploading the document via FTP
- Screenshot of the document
- Copy and paste content onto another document
- Posting content on social networks such as Facebook or LinedIn

In addition to what is implemented through the IT tool, in order to prevent documents from being disclosed, staff in production departments are prohibited from accessing with mobile devices equipped with a camera.

In addition, the possibility of making photocopies of any kind has been regulated through the adoption of a special software solution that tracks who and when has created a hard copy of the document.

Internal Security: Antivirus Client Endpoint

Each server and each client station residing within the Archiva network is equipped with an endpoint antivirus system, centrally managed by a specific dedicated server and controlled by an Archiva operator; this centralised management allows the distribution of updates and behavioural policies towards any detected threats.

2.2.9 Ethics, transparency and fairness

Archiva is inspired by and observes the principles of loyalty, correctness, transparency, efficiency and all the operations and negotiations carried out in the performance of its activity are inspired by the utmost correctness, completeness and transparency of the information, legitimacy under the formal and substantial aspect and clarity and truthfulness of the accounting documents according to the regulations in force and the internal procedures.

Corrupt practices, illegitimate favours, collusive behaviour, solicitation, directly and/or through third parties, of personal and career advantages for oneself or others, are prohibited without exception.

It is never permitted to pay or offer, directly or indirectly, payments, material benefits or other advantages of any kind to third parties, government representatives, public officials and public or private employees, in order to influence or compensate them for an act of their office.

Acts of commercial courtesy, such as gifts or forms of hospitality, are permitted only if they are of modest value and, in any case, do not compromise the integrity or reputation of either party and cannot be interpreted by an impartial observer as aimed at acquiring improper advantages.

Anyone who receives proposals for gifts or favourable treatment or hospitality which do not constitute acts of commercial courtesy of modest value, or the request for such from third parties, shall reject them and immediately inform their superior, or the body to which they belong, and the Supervisory Board.

Archiva informs third parties of the commitments and obligations imposed by the Code, requires them to respect the principles that directly concern their activity and takes the appropriate internal and, if within its competence, external initiatives in the event of non-compliance by third parties.

2.3 Protection of health, safety, the environment and public safety

Archiva's activities shall be conducted in accordance with international agreements and standards and with laws and regulations relating to the protection of the health and safety of workers, the environment and public safety.

Archiva actively contributes to the promotion of scientific and technological development aimed at safeguarding resources and the environment. The operational management refers to criteria of environmental protection and energy efficiency, pursuing the continuous improvement of the conditions of health and safety at work and environmental protection.

Archiva's employess, within the scope of their duties, actively participate in the process of risk prevention, of safeguarding the environment and public safety and of protecting the health and safety of themselves, their colleagues and third parties.

2.4 Confidentiality and protection of business secrets

Archiva's activities constantly require the acquisition, storage, processing, communication and dissemination of news, documents and other data pertaining to negotiations, administrative procedures, financial operations, know-how (contracts, deeds, reports, notes, studies, drawings, photographs, software, etc.) which, by contractual agreements, cannot be made known to the outside world or whose inappropriate or untimely disclosure could damage the company's interests.

Without prejudice to the transparency of the activities carried out and to the information obligations imposed by the provisions in force, it is the obligation of the Persons of Archiva to ensure the confidentiality required by the circumstances for each piece of information learnt by reason of their working function.

The information, knowledge and data acquired or processed during one's work or through one's duties belong to Archiva and may not be used, communicated or divulged without specific authorisation from one's superior in a hierarchical position in accordance with specific procedures.

2.5 Protection of privacy

Archiva complies with the provisions of Legislative Decree no. 196 of 30 June 2003 "Code for the protection of personal data" as well as fully respecting professional secrecy, also guaranteeing absolute security and confidentiality through both computer and telematic tools designed to store, manage and publish the data themselves exclusively on the basis of the contracts stipulated.

To this end, Archiva has implemented an Information Security Management System certified by the RINA Certification Body in accordance with the international standard UNI CEI ISO/IEC 27001:2013, to guarantee the availability, integrity and confidentiality of the data processed.

In the event of a disaster that compromises the availability of the main office and the services cannot be provided, Archiva has implemented a Disaster Recovery solution, at a facility located over 100 km away, from which the services of document consultation and reception of digital flows are guaranteed within 6 hours of the declaration of the emergency situation.

Archiva intends to guarantee that the processing of personal data carried out within its structures is carried out in compliance with the fundamental rights and freedoms, as well as the dignity of the persons concerned, as provided for by the regulations in force.

The processing of personal data must take place in a lawful and correct manner and, in any case, only data necessary for specific, explicit and legitimate purposes are collected and recorded. In the storage of data, Archiva undertakes to adopt suitable and preventive security measures for all databases in which personal data are collected and stored, to avoid risks of destruction and loss or unauthorised access or processing.

Archiva personnel are required to:

- acquire and process only such data as are necessary and appropriate for the purposes directly connected with their functions and responsibilities;
- acquire and process the data only within specific procedures and store and archive them in such a way that unauthorised persons are prevented from gaining knowledge of them;
- to represent and order the data in such a way that any person authorised to have access to them can easily gain as accurate, comprehensive and truthful a picture as possible;
- communicating the data within the framework of specific procedures or upon express authorisation of the superior positions and, in any case, only after having verified that the data are not covered by confidentiality clauses.

2.6 Human Resources

Archiva undertakes to develop the skills and competences of the management and of the employees, so that, within the work performance, the energy and the creativity of the individuals find full expression for the fulfillment of their potential, and to protect the working conditions both in the protection of the psycho-physical integrity of the worker and in the respect of his dignity.

The motivation and professional growth of employees are the key to success. Respect, trust, fairness and dialogue are the principles that inspire Archiva to create enthusiasm and team spirit.

Unlawful conditioning or undue hardship is not allowed and working conditions that allow the development of the person's personality and professionalism are promoted.

Archiva takes particular account of the recognition and protection of the dignity, freedom and equality of human beings, the protection of labour and trade union freedoms, health, safety and the environment, as well as the system of values and principles relating to transparency and sustainable development.

In Archiva, relations at all levels must be based on criteria and behaviour of honesty, correctness, collaboration, loyalty and reciprocal respect and in no way may the conviction of acting to the advantage or in the interest of Archiva justify, even in part, the adoption of behaviour in contrast with the principles and contents of the Code.

2.7 Suppliers and external collaborators

Archiva undertakes to seek in its suppliers and external collaborators suitable professionalism and commitment to sharing the principles and contents of the Code and promotes the building of lasting relationships for the progressive improvement of performance in the protection and promotion of the principles and contents of the Code.

In relations of tender, procurement and, in general, supply of goods and/or services and external collaboration (including consultants, agents, etc.), Archiva's People are obliged to

a. observe the internal procedures for the selection and management of relations with suppliers and external collaborators, and not to preclude any subject in possession of the required requisites from competing for a supply contract with Archiva;
b. adopting only objective evaluation criteria in the selection process, in a declared and transparent manner;
c. include in contracts a confirmation that they have read the Code and an express obligation to abide by its principles.

The remuneration to be paid shall be exclusively commensurate with the performance specified in the contract and payments shall in no way be made to a person other than the other party to the contract or in a third country other than that of the parties or of performance of the contract.

2.8 Corporate security

All the Archiva personnel are obliged to contribute actively to the maintenance of an optimal standard of company security, refraining from illegal or in any case dangerous behaviour and reporting to their own superior or to the body of which they are part, any activity carried out by third parties to the detriment of the assets or human resources of Archiva.

In any context that requires particular attention to one's personal safety, one is obliged to scrupulously comply with the indications provided by Archiva, refraining from behaviour that may put one's own and others' safety at risk, and promptly reporting to one's superior any situation that endangers one's own safety or that of third parties.

3 Tools for applying the Code of Ethics

3.1 Internal control system

Archiva undertakes to promote and maintain an adequate system of internal control, to be intended as a set of all the instruments necessary or useful to direct, manage and verify the activities of the company with the aim of ensuring the respect of the laws and of the company procedures, of protecting the company assets, of managing in an optimal and efficient way the activities and of supplying accurate and complete accounting and financial data.

The responsibility for implementing an effective internal control system is common to every level of Archiva's organisational structure; consequently, all the personnel of Archiva, within the scope of their functions and responsibilities, are committed to defining and actively participating in the correct functioning of the internal control system.

Everyone is the responsible custodian of the company assets assigned (tangible and intangible) which are instrumental to the activity carried out; no employee may make, or allow others to make, improper use of the assets assigned and of Archiva's resources.

Practices and attitudes relating to the commission or participation in the commission of fraud are prohibited without exception.

The Supervisory Board and the Board of Statutory Auditors have free access to data, documents and information useful for carrying out their activities.

3.2 Transparency of accounting records

The administrative area of Archiva is equipped with controlled access through magnetic badges enabled only for the administrative staff, for the Administrative, Financial and Personnel Director and for the Managing Director.

Accounting transparency is based on the truth, accuracy and completeness of the information underlying the relevant accounting records. Each member of the corporate bodies, management or employee is obliged to cooperate, within the scope of his or her competences, in order to ensure that management facts are correctly and promptly represented in the accounting records.

It is forbidden to behave in such a way as to undermine the transparency and traceability of financial reporting.

Adequate supporting documentation of the activity carried out shall be kept on file for each transaction:

- easy and timely bookkeeping;
- identification of different levels of responsibility and division of tasks;
- the accurate reconstruction of the operation, also to reduce the likelihood of errors, including material or interpretative errors.

Each record must reflect exactly what the supporting documentation shows. It is the task of the administrative staff to ensure that the documentation is easily traceable and ordered according to logical criteria.

The Persons of Archiva who become aware of omissions, falsifications, negligence in the accounts or in the documentation on which the accounting records are based, are obliged to report the facts to their superior, or to the body of which they are part, and to the Supervisory Body.

3.3 Scope and reference structures of the Code of Ethics

The principles and contents of the Code of Ethics apply to the activities carried out by Archiva and to all the personnel of the company.

It is primarily the task of the Directors and Management of Archiva to give concrete form to the principles and contents of the Code, taking on the responsibilities both internally and externally, representing with their own behaviour an example for their own collaborators in the observance of the Code, urging them to formulate questions and suggestions regarding the single provisions.

Archiva personnel are required to be familiar with the principles and contents of the Code as well as with the reference procedures governing the functions and responsibilities covered.

It is the obligation of each Archiva Person to:

- refrain from conduct contrary to these principles, contents and procedures;
- require from third parties with whom Archiva operates, confirmation that they have taken cognisance of the Code of Ethics;
- promptly report to its own superiors about possible cases or requests of violation of the Code; reports of possible violations are sent in compliance with the operating procedures established by the specific procedures established by the Board of Auditors and by the Supervisory Body of Archiva S.r.l.;
- cooperate with the Supervisory Board in the verification of possible violations;
- take immediate corrective action when required by the situation and, in any case, prevent any kind of retaliation.

3.4 Code of Ethics, Supervisory Board pursuant to Legislative Decree no. 231/2001

The Code of Ethics represents, among other things, a non-derogable general principle of the Organisational, Management and Control Model adopted by Archiva S.r.l., pursuant to the Italian regulations on the "liability of entities for administrative offences dependent on crime" contained in Legislative Decree no. 231 of 8 June 2001.

Archiva S.r.l. assigns to the Supervisory Body established on the basis of the Organisational Model the functions of Guarantor.

The Supervisor is assigned the tasks of:

- promote the implementation of the Code and the issuing of reference procedures;
- report and propose useful initiatives for the greater dissemination and knowledge of the Code, also in order to avoid the repetition of proven violations;
- promote communication and specific training programmes for Archiva's management and employees;
- examine reports of possible violations of the Code, promoting the most appropriate checks;
- informing the structures of the competent areas of the results of the checks relevant for the adoption of any sanctioning measures; informing the structures of the competent areas of the results of the checks relevant for the adoption of appropriate measures.

Information and reports should be sent to the Supervisory Body in writing to the e-mail address odv@.archivagroup.it.

The Supervisory Body of Archiva S.r.l. also submits to the Board of Auditors as well as to the President and the Managing Director, who report to the Board of Directors, an annual report on the implementation and the possible need to update the Code.

Each information flow is addressed to the Supervisory Board's e-mail box.

The Code is made available to all Archiva personnel in compliance with the applicable regulations and can also be consulted on Archiva S.r.l.'s internet and intranet sites.

The revision of the Code is proposed by the Supervisory Body and approved by the Board of Directors of Archiva S.r.l..

Compliance with the rules of the Code shall be considered an essential part of the contractual obligations of all Archiva's Persons under and pursuant to applicable law.

Violation of the principles and contents of the Code may constitute a breach of the primary obligations of the employment relationship or a disciplinary offence, with all the consequences of the law, including with regard to the preservation of the employment relationship, and lead to compensation for any damages arising therefrom.

Legal and operational headquarters
Via Spagna, 24
37069 Villafranca (VR)
T +39 045 2880 000
F +39 045 2880 001
archivagroup.it

Share capital: Euro 500,000.00
REA of VR: 319751 Registered in the Verona Register of Companies Tax code and VAT number 03237470236