Worldline

DIGITAL PAYMENTS
FOR A TRUSTED WORLD

ARCHIVING POLICY OF EAS

TSP MediaCert

AUTHOR(S) : Guillaume Bailleul
DOCUMENT NO : WLM-ARC-F210
VERSION : 1.3
STATUS : Final
SOURCE : Worldline
DATE OF THE DOCUMENT : June, 2020
NUMBER OF PAGES : 30

Rôle	Nom	Signature	Date
Reviewer1 – TSP Assitant Resp	Fanny Lesecq	Fanny Lesecq	2019/12/23
Reviewer 2 – RSSI	Didier Sobkowiak	Didier Sobkowiak	2019/12/23
Quality Assurance Function	Fanny Lesecq	Fanny Lesecq	2019/12/23
Document owner	Comité Mediacert	Guillaume Bailleul	2019/12/23
Approver – TSP Resp	Guillaume Bailleul	Guillaume Bailleul	2019/12/23

Table of Contents

List of changes

Version	Date	Description	Author(s)
1.0	2012/12/07	Initial version	Jean Jacques Milhem
1.1	2018/10/05-2018/12/10	Review and amendment	Guillaume Bailleul
1.2	2018/12/12–2019/31/03	Amendments following the certification audit	Guillaume Bailleul
1.3	2019/23/12	Reformulation of §6.1.3.2 Update of the graphic charter	F.Lesecq

1 Introduction

1.1 Purpose of the document

This document describes the Archiving Policy (AP) of WL e-archiving, an Electronic Archiving System (EAS) hosted by Worldline.
This document serves as a basis for the development of AP to be implemented as part of the provision of an Archiving Service.
The ultimate objective of the AP is to enable the Electronic Archives managed by the EAS that have an initial legal value to be considered reliable, i.e. to maintain their integrity and guarantee that they conform to the original documents, both in terms of probative value and validity, throughout their retention period within WL e-archiving.

1.2 Name and Coding

This document is entitled "WL e-archiving Policy. ». It is referenced in the document system under the reference WLM-ARC-F210. This Archiving Policy is identified by OID 1.2.250.1.111.20.4.1.

1.3 Bibliography

1.3.1 External References

Reference	Description
[GA Z42-019]	GA Z42-019 (June 2010) AFNOR Application guide for NF Z 42-013
[NF 461]	NF 461 (September 2015) AFNOR Certification Certification rules for an electronic archiving system
[NF Z 42-013]	NF Z 42-013 (March 2009) AFNOR Electronic archiving: specifications relating to the design and operation of computer systems to ensure the preservation and integrity of the documents stored in those systems.
[RGPD]	General Data Protection Regulations European Parliament and Council of the EU
[ISO 9001]	ISO 9001 (2015) Quality management systems
[ISO 27001]	ISO 27001 (2013) Information technology - Security techniques - Information security management systems - Requirements

1.3.2 Internal References

Reference	Description
[AR]	Risk Analysis of the Archiving Platform Electronic Archiving Service Reference : WLS-ARC-F191
[DDTS] **[QAP]**	SAE WA System Technical Description File Electronic Archiving Service Reference : WLS-ARC-F208 Software Factory Quality Assurance Plan TSP Mediacert Order No.: WLM-SFY-F122
[GP]	MediaCert TSP General Policy TSP Mediacert Order No.: WLM-TSP-F094 OID: 1.2.250.1.111.20.1.1
[ISP]	Worldline France Information Security Policy Worldline France Order No.: WLM-SEC-F002
[OSP]	Operational Security Policy Electronic Archiving Service Reference : WLS-ARC-F206
[QMS]	Worldline Quality Management System Worldline France Order No.: WLM-QUA-F000
[ISMS]	Worldline Information Security Management System Worldline France Order No.: WLM-SEC-F002

2. Definitions

2.1 Definitions

2.1.1 Digital Document

The Digital Document is a set of content, logical structure and presentation attributes. This set allows the representation of the document in a human-intelligible form. The digital document is understood in the sense of the definition provided in [NF Z 42-013].

2.1.2 Archive

An Archive is a package of information composed of one or more computer files received, stored and communicated by WL e-archiving. The information packet is the association of the content and its perpetuation attributes specifying its origin, its context, its identification and the attributes allowing the control of its integrity. It is also referred to as e-archiving.

2.1.3 Metadata

A structured set of technical, management and descriptive information attached to a record that describes the characteristics of the record to facilitate its retrieval, management, access, use or preservation.

2.1.4 Electronic Archiving

[NF Z42-013]Electronic Archiving is defined as all actions aimed at identifying, collecting, filing, storing, communicating and restoring electronic documents, for the duration necessary to meet legal obligations or for information needs or for heritage purposes.

2.1.5 Archiving Authority

The Archiving Authority is the business entity responsible for the management of the archive service. This entity offers services, which can be shared, based on a global electronic archiving service provided by a Third Party Archiver.

2.1.6 Customer

The Customer is the project owner, or, for the public sector, the entity that may have a legal structure of grouping to offer mutualized archiving services to its member members for their own archiving authorities.

2.1.7 Footprint

The Footprint is the result of the application of a canonical formatting function and then a hash function applied to a document. This result is a set of bytes allowing characterizing a document. Any modification of the document will result in a different hash that will reveal the modification by comparison with the first hash.

2.1.8 Archive Description File

The Archive Description File is a constituent file of the Archive containing all the metadata of the Archive or the documents contained in the Archive.

2.1.9 Time stamping of a document

Time stamping is a mechanism for associating a date and time with an event, a document or a piece of computer data. Its purpose is generally to record the time at which an operation was performed.

2.1.10 Unique Archive Identifier

The Unique Archive Identifier (UAI) is the identifier of the Archive whose uniqueness is guaranteed for a given Archive Agreement.
The pair consisting of the Archive Agreement ID and the UAI is unique across the Archive Service platform.

2.1.11 Restitution

A set of mechanisms for retrieving and delivering digital records to the producing organization or its constituents and then destroying them within its archival system.

2.1.12 Deposit

Transmission by a client of a digital document to the EAS

2.1.13 Archiving Service

The Archiving Service designates the entity to which the payment is made. It is responsible for the management of the Archives paid by the Depository Services, intended to be communicated to the Users of the Depository Services / Producers in compliance with the communication deadlines. The Archiving Service also provides consulting services to the Paying Services or Producer Services.

2.1.14 Control Department

In the public domain, the Control Service is made up of persons authorized by the legislative and regulatory texts in force to control the Public Archives, in particular the way in which the Archiving Authorities carry out their mission (creation, deposit, storage, communication of the Archives, administration). Controllers must have access to WL e-archiving.

2.1.15 Producer Service

The Producer Service is the entity that initially received or produced the Archive and owns it. The notion of Service Producer is specific to the public domain.

2.1.16 Depositing Service

The Upload Service is the entity that uploads a packet of information to an Archiving Service.

2.1.17 User

The User is a natural or legal person authorized to consult the Archives kept on the EAS in accordance with the applicable legislation on communication of the Archives.

2.1.18 User

The User designates any individual or legal entity authorized to use WL e-archiving.

2.1.19 Third Party Archiver

A Third Party Archiver is a natural or legal person in charge, on behalf of third parties, of offering the functionalities of the Electronic Archiving Service, namely: receipt of deposits, conservation, communication, destruction or restitution. The conditions for carrying out these services must be defined in a service contract in accordance with the recommendations of the standard [NF Z42-013] and the application guide [GA Z42-019]. In the present AP, this is Worldline.

2.1.20 Archiving Agreement

The Archiving Convention is a document describing all the rules for the transfer, control and conservation of archives. This document is shared between the client and the Third Party Archiver.
Each Archiving Agreement is archived within WL e-archiving, for an indefinite period of time.

2.1.21 Business Continuity Plan (BCP)

A set of measures designed to ensure, under various crisis scenarios, including in the face of extreme shocks, the maintenance, if necessary temporarily in a degraded mode, of the company's essential services and then the planned resumption of activities.

2.2 Abbreviations and Acronyms

Acronym	Description
AA	Archiving Authority

UAI	Unique Archive Identifier
UAAI	Unique Archiving Approval Identifier
ADF	Archive Description File
OH	Operational Handbook
AP	Archiving Policy
OSP	Operational Security Policy
EAS	Electronic Archiving System, corresponds to WL e-archiving
SOP	Standard Operation Procedure
PS	Producer Service
DS	Depositing Service
TA	Third Party Archiver

3. Features implemented

The Third Party Archiver offers an Electronic Archiving Service for digital documents called WL e-archiving. This service is secure. It is committed to Customers who have subscribed to the service at:

- to be integrated into the EAS, by securing the transfer of digital records;
- retain these documents and ensure that they can be guaranteed for the contractually agreed retention period:
  - their safety;
  - their durability;
  - their integrity;
  - their traceability;
  - their online availability and accessibility to Authorized Users;
- Respect the Client's requests for reversibility at the end of the contract in accordance with the contractual agreements between the parties.

WL e-archiving is also referred to as the Archiving Service in this document.

3.1 Payment

3.1.1 Checking the origin of the payment

The Third Party Archiver ensures the provenance of the Digital Documents. The Third Party Archiver references the sources of documents for each of its Clients. The Third Party Archiver secures the means of communication. He ensures the confidentiality of the exchanges and the authenticity of the sources.

3.1.2 Digital documents and metadata

Digital records that are intended to be preserved over time are accompanied by a set of metadata necessary for that preservation. Digital records are also referred to as documents.

3.1.3 Unique Archive ID

Refer to the Definitions chapter.

3.1.4 Format validation

WL e-archiving guarantees the preservation of documents. In order to reinforce the preservation capacities of a digital document, the Archiving Service offers an optional format validation service.

The Service Agreement defines the list of formats validated by the Third Party Archiver.

3.1.5 Timestamp

The date (date and time) of the creation of the Archive is kept and sealed in the Archive. This date is based on a standardized time service with several time sources.

3.1.6 Sealing the Archive

The Archive is sealed by cryptographic means to ensure the integrity of the Archive's records and the metadata describing it.
The Archive and Archival Mark calculations are performed using a cryptographic hash function.
The print is sealed. Refer to the Sealing chapter of this document.
The seal of the Archive contains a time countermark to prove the existence of the Archive on a given date.
The Sealed Archive contains, among others, the following attributes:

- the unique identifier of the Archive ;
- the creation date of the Archive ;
- the Mark of each of the documents in the Archive;
- descriptive metadata for each of the records in the Archive;
- the descriptive metadata of the Archive.

3.1.7 Indexing the Archive

During the constitution of the Archive, all the metadata is extracted in order to allow the indexing of the Archive and to simplify searches.
The metadata in this set can be used for searching when consulting Archives (see 3.2.2).

3.1.8 Securing the Archive Storage

Following its constitution, the Archive is deposited on several remote sites in order to guarantee its security. The storage solutions used at each site guarantee multiple copies of the Archive in order to secure the storage against the risk of hardware failure.
An asynchronous backup copy is made on a backup solution.
The Archiving Service offers a functional acknowledgement guaranteeing the security and storage of the Archive.

3.1.9 Proof of deposit of the Archive

3.1.9.1 Technical Acknowledgement

Upon deposit, a technical acknowledgement of receipt is returned by the Archiving Service. It certifies that the Archive has been completely received and that the archiving request is complete and consistent.

Receipt of this acknowledgement of receipt ensures that the Archive has been properly **constituted and sealed**. The Archive thus becomes accessible to its owner through the tools provided for this purpose.
This technical acknowledgement of receipt contains, among other things, the following information:

- The unique identifier of Archive ;
- Drop-off time;
- The status of the archive;
- The location of the archive;

3.1.9.2 Functional acknowledgement of receipt

After deposit, a functional acknowledgement of receipt is available upon request. It can be accessed using the Archive's unique identifier and returns the same information as the technical acknowledgement of receipt. It guarantees the **security of the Archive,** i.e. the Archive is stored on the sites defined by this archiving policy.
The depositor then has proof of deposit for each archive.

3.2 Search

WL e-archiving offers two types of research:

- search by Unique Archive Identifier ;
- Multi-criteria search.

3.2.1 Search by Unique Archive Identifier

WL e-archiving offers a way to search the Archives according to their UAI. The search tool is only accessible to Users defined by the Client.
For a given User, the search results contain only the Archives to which the User has access in accordance with the Archiving Agreement.

3.2.2 Multi-criteria search on metadata

WL e-archiving provides a way to search for Archives based on the metadata associated with the Archive or content at the time of deposit. The search tool is only accessible to Users defined by the Client.
For a given User, the search results contain only the Archives to which the User has access in accordance with the Archiving Agreement.

3.3 Communication

3.3.1 Unit communication

When in possession of an UAI, the User can retrieve the following information:

- the journal of the Archive;
- the sealing attributes of the Archive ;

- the description of the Archive;
- each of the constituent contents of the Archive.

All this information can be downloaded from a client application authenticated by the Archiving Service.

3.3.2 Communication in lot

On special request and under the conditions provided for in the service agreement, it is possible to ask the Archiving Service for a communication from a large number of Archives.

3.4 Archive Modification

WL e-archiving does not allow modification of the Archive and guarantees its integrity. Nevertheless, in certain contexts, it may be necessary to evolve the content. The Archiving Service allows the deposit of a new revision of the Archive referring to the previous version. Therefore, by default, the last revision of the Archive will be returned when the communication is made.
Optionally, and depending on the archiving agreement, previous versions of the Archive may be deleted to ensure compatibility of the service with the General Regulations for the Protection of Personal Data (GDPR). The Archive Log then keeps a record of the deletions of previous versions.

3.5 Restitution

The Archives may be returned in full at the Customer's request. The methods of application of this restitution will follow the constraints and recommendations of the restitution in number (see 3.3.2).
The definition of the return medium is defined in the service agreement and is made in agreement with the Customer.
The default output format is a specific WL e-archiving format inspired by recognized formats.

3.6 End of life of the Archive

The service agreement provides for a length of service and a retention period for archived documents.

3.7 Exceptional Archive Destruction

The Customer may, upon express request, request the destruction of the Archives. In this case, the Archives concerned by the destruction must be clearly identified. A record of the request and of the deletion will be kept by the Archive Service.
Deleting an archive involves deleting its metadata while retaining its logs.

3.7.1 Service life cycle

Regularly the Archives are checked in order to compile a list of Archives whose life (duration of conservation) is coming to an end. This list is communicated to

the person in charge (Client) of the Archives who, for all or for each of them, will determine the next step in the life of the Archive, either to authorize the destruction or to extend the life of the Archive.
The Archiving Service keeps track of the choices and carries out the necessary actions.

3.7.2 Conservation

3.7.2.1 Duration of conservation

The storage period is defined in the contract between the Customer and the Archiving Service. For each type of Archive defined in the archiving agreement an archiving duration is defined.
In the event of termination of the contract, a complete return of the Archives will be planned (see 3.5).

3.7.2.2 Consultation beyond the term of service

If provided for in the contract, access to the Archives may be maintained after the termination of the depository service. The Client may access the Archives in accordance with the conditions set out in the contract.
The Customer may request the return in accordance with the conditions provided for in the contract and according to the constraints defined in the archiving policy (see 3.5).

3.8 Operations

3.8.1 Operating procedures and rules

All WL e-archiving procedures and rules are documented. In accordance with [ISMS] rules, they are subject to regular review and continuous improvement.

3.8.2 Systems Development

The development, integration and testing of new systems, or new versions of existing systems, are separated (tasks and physical environment) from operational activities. Developed deliverables are installed in production from the documented repository.

3.8.3 System maintenance

Maintenance operations on operating systems are prepared and recorded. The procedures for intervention on the systems (hot or cold) are formalized and the elements subject to maintenance are tested in a separate environment before being put into operation.
Maintenance operations are carried out under the control of personnel with trusted roles, as defined in the General Policy [GP] document.
Maintenance operations are fully traceable.

3.8.4 Media Management

The storage media (computer and paper) are subject to a formalized management in accordance with the security and quality needs of the Mediacert

Trust Service Provider (TSP). The rules applicable to the Mediacert TSP services are set out in the General Policy [GP] document.
In particular, the reuse / disposal / removal from the premises (maintenance) of media is subject to strict procedures related to the secure deletion of files contained on the media or the physical destruction of the media.

3.8.5 Reporting

The Archiving Service provides Customers with a monthly activity report containing the measures necessary to manage the activity. The following will be present in particular

- the number of Archives deposited over the period ;
- the size of the storage space used.

3.9 Certificates available

For each archive present in the archiving system, the Third Party Archiver can provide several types of certification to attest to the functioning of the system and the respect of the archive's life cycle.

These attestations are as follows:

- The certificate of copy of an archive provides all the necessary elements to ensure that the archive communicated is complete and compliant.
- The archive deletion certificate enables archive deletions to be traced on the archiving platform.
- The certificates of creation, deletion and modification of an archiving agreement make it possible to trace the life cycle of a Client's archiving agreements.

The Certificate of Execution of the Background Check reports on the continuous checks of the archive background.
Archive life cycle attestations are grouped together and signed periodically at fixed and configurable intervals to form the log.

4. Organizational principles

4.1 Archiving policy

4.1.1 Dissemination of the Archiving Policy

The Archiving Policy is a public classified document disseminated, on request, to all parties concerned by the EAS on the project's document space.

4.1.2 Evolution of the Archiving Policy

The Archiving Policy is kept up to date for any changes to the EAS. Archiving Practice Statements (APD) must be maintained in accordance with the current AP.
The AP is reviewed, at least annually (see recurrent action WLP-TSP-F106).

4.1.3 Enforcement of the Archiving Policy

The Third Party Archivist shall plan and implement the procedures and means necessary to ensure the application of the AP.

4.2 Conservation of the Archives

During the entire retention period, the Third Party Archiver may present the Archive or a part of the Archive referenced by a Unique Archive Identifier (UAI).
To ensure preservation, several copies of the Archive are made according to the rules specified in the Archiving Practice Statement.
A technical acknowledgement is issued upon complete receipt of the Archive and its sealing.
A functional acknowledgement is issued as soon as the number of copies matches the rules defined in the CCA.
Regular processes ensure, by sampling, the integrity of the Archives held by the Third Party Archivist.

4.2.1 Service Availability

The WL e-archiving service is designed for 24/7 availability outside of scheduled maintenance periods. The availability rate provided is 99.5%. The technical architecture of the EAS, defined in the [DDTS], ensures a high level of availability.

4.2.2 Archive Security

The essential aspects of securing the storage of digital documents are also dealt with:

- sustainability ;
- integrity;
- confidentiality ;
- traceability ;

- Reversibility.

4.2.2.1 Sustainability

The document storage system used ensures that each hardware component of the platform is always in good working order. In the event of failure of a hardware component, the redundancy principles put in place ensure continuous access to the archive despite the failure and a return to the number of copies required after replacement of the defective component.

4.2.2.2 Integrity

The sealing of the Archive as well as the Digital Mark of the various components of the Archive are regularly checked by a continuous control of the Electronic Archiving System.

4.2.2.3 Privacy

The Third Party Archiver undertakes not to analyze the information contained in the archived documents.
According to the Archiving Authority's Archiving Convention, format validators may be used to ensure the validity of the format of the deposited document. In this case, only the structure of the document is analyzed, the content is neither extracted nor analyzed.
WL e-archiving implements partitioning and authorization management to ensure that only authorized Users access the Archives.
In some cases, the Depositing Service can encrypt documents before they are deposited in the archive. This principle allows for enhanced confidentiality, but implies control by the Client of the life cycle of the encryption keys used.
The archives are encrypted before they are sent to the storage facility.

4.2.2.4 Traceability

The Archiving Service ensures traceability by setting up a logging system. System events are recorded in different logs.
The following types of logs are defined in the system:

- Archives Life Cycle Journal ;
- event log ;
- system log.

Archive Life Cycle Journal

The system records for each Archive the events concerning its life cycle. These events include, but are not limited to, the following:

- deposit of the Archive ;
- deleting the Archive ;
- modification of the lifetime of the Archive ;

- Restitution of the Archive.

The log of an Archive is accessible to Archive Users according to the same rules as access to the Archive.

Event Log

There is a recording system to list events concerning the resources of the WL e-archiving platform. It lists the following events:

- adding material ;
- hardware replacement ;
- Maintenance.

These elements are accessible to the platform operators.

System Log

System logs are a subset of event logs. They are treated with the same level of security as event logs. They record all the events of the platform. They are listed, among others:

- safety actions ;
- the evolutions of the system ;
- Access to the platform.

These logs allow an a posteriori analysis and reconstruction of the platform's history.

4.2.2.5 Reversibility

WL e-archiving respects the principle of reversibility (see 3.5). The archived documents and their metadata are not modified by the processes of the Archiving Service.
The Archiving Service therefore allows the restitution of documents and their metadata without any internal transformation.
The Archives will be restored in a specific format for the Archive Service inspired by market standards. The medium of the restitution is defined in the contract.
The restitution process will be conducted according to the conditions set out in the contract.

5. Principles of implementation

Security is one of the crucial points of WL e-archiving. The security of the Information System is based on the general rules put in place in the company to obtain the necessary certifications for this type of activity. System security concerns:

- network security (filtering, use of private networks) ;
- securing physical access ;
- securing logical access (personal authentication, use of certificates, access security policy);
- securing exchanges (use of encrypted transport, HTTPS, TLS);
- securing the operation (definition of procedures, standardization) ;
- securing developments (application of a Quality Assurance Plan [QAP]).

The principles implemented by the Third Party Archiver comply with all the rules defined in the [ISMS] and Worldline's [QMS] in order to guarantee a sufficient level of security. The following elements provide information on their implementation.

5.1 Documentation management

The document management policy in place is described in the General Policy [GP] and is consistent with the Quality Management System [QMS] implemented in the company. The company is certified ISO 9001 [ISO 9001].

5.2 Security Management

Security management is based on the global approach implemented for all Mediacert TSP Trust Services and on a similar approach implemented globally in the company.

5.2.1 Information security policy

The policy implemented is described in the General Policy [GP] and complies with the Information Security Management System [ISMS] implemented in the company. The company is certified ISO 27001 [ISO 27001].
Specific rules or the specialization of certain rules are defined in the Operational Security Policy [OSP] specific to WL e-archiving.
The Information Security Policy [ISP] expresses, among other things, the description of relationships with suppliers.

5.2.2 Business Continuity Planning (BCP)

The Third Party Archiver has a Business Continuity Plan (BCP) covering the perimeter of the EAS. The Business Continuity Plan is carried out according to the need to maintain the integrity of the Archives, in particular the non-loss of archives. The procedures defined in the various plans must make it possible to maintain the activities of the Archiving Service in accordance with the needs for integrity and continuity.

This plan is regularly updated. It describes a set of measures to be applied with the aim of maintaining, sometimes in a degraded form, the functionalities of WL e-archiving.

5.2.3 Physical and Environmental Security

WL e-archiving is based on a technical platform distributed over 3 distinct sites. Each site, one of which is more than 400 kilometer away, has its own operating resources (air conditioning, power supply, back-up generator).

5.2.4 Access security

5.2.4.1 Physical access security

Access to EAS assets is restricted and strictly controlled. Access to the assets of the EAS is restricted and strictly controlled and follows security rules defined in the [ISP].

5.2.4.2 Logical access security

Logical access to EAS assets is restricted and strictly controlled. In accordance with the [ISP], access is by name and tracked, and is subject to regular verification of access authorizations.

5.2.5 Safety of equipment

The choice of the equipment, their installations and their operation is made following the global rules defined in the Third Party Archiver's company.

5.2.6 Incident Management

Each entity involved in the Electronic Archiving Service defines the organization and procedures to be followed in the event of a security incident. The procedures to be followed in the event of an incident are defined in Standard Operating Procedure (SOP) sheets.
The feedback of information to the Client follows the standard procedures defined in the company.

5.2.7 Software security

5.2.7.1 Software Development

Software development follows the rules defined in the Quality Assurance Plan [QAP] of the department in charge of the archiving platform. This QAP is compatible with the company's Quality Management System and Information Security Management System.

5.2.7.2 Software Integration

In accordance with the company's best practices, the Third Party Archiver implements test and acceptance systems to ensure the correct functioning

of the service during the evolution of the company's software components.

5.2.8 Information System Security

In accordance with corporate best practices and the [ISMS], the Third Party Archiver implements a secure platform by ensuring redundancy of critical elements to ensure the security of the electronic records management system.

5.2.9 Human Aspects

5.2.9.1 Training and Awareness Raising

During its integration, the new staff is trained and made aware of the particular nature of the security of the Third Party Archiver's job. They are also made aware of the company's security policy.

5.2.9.2 Job description

The work of any staff working on WL e-archiving, at any level (operator, administrator, maintenance, etc.) is subject to a job description defining the roles, obligations and responsibilities of the staff concerned.

5.3 Exchanges between the Customer and the Third Party Archiver

5.3.1 Project Exchange

The Third Party Archiver does not offer a steering meeting or project monitoring centralized on the Electronic Archiving Service with the Customer. As the use of archiving is usually part of a larger IT project, instances for such follow-ups exist. Archiving monitoring is integrated into each of these instances. At the request of the Client and the Worldline Project Managers, a representative of the Third Party Archiver may participate.

5.3.2 Technical Exchange

Exchanges of data flows between the Customer and the Third Party Archiver are made through secure communication links. The nature of the links will be defined in an agreement between the Customer and the Third Party Archiver. The securing of the links is the result of joint work between the technical teams of the Customer and the Third Party Archiver.
The links can be specialized links or internet links. The operation of the link to the archiving platform is the responsibility of the Customer.

5.3.3 Evaluation of the quality perceived by the customer

The measurement of the quality perceived by the Customer is made through the measurements carried out by the company. The company's [QMS] specifies how the perceived quality of the CSAT process is measured. The Third Party Archiver analyzes the results of these returns and implements action plans when necessary.

6. Technical principles

6.1 Identification of actors

The archiving policy defines the following roles; the responsibilities of each are described in the following sections of the document:

- the Client;
- the Third Party Archiver (TA);
- the Archiving Authority (AA) ;
- the Producer Service (PS) ;
- the Depositing Service (DS) ;
- the Service Control (SC).

6.1.1 The Third Party Archiver (TA)

6.1.1.1 AHR liability

The TA is responsible for writing, updating and distributing the WL e-archiving AP. This AP, referenced by the contract, defines the commitments of the entities concerned for the delivery of the Electronic Archiving Service provided by WL e-archiving.

The commitments made by the Third Party Archiver to his Customer are defined in a contract or its annexes (archiving agreement). Must be present or referenced:

- the service description agreed with the Customer;
- the commitments on the quality of service agreed with the Customer;
- a technical annex describing the system interfaces and methods of access to the service ;

-
- a financial schedule detailing the financial terms and conditions for the provision of the service.

6.1.1.2 Responsibility of the TA

The TA is responsible for its obligations under the AP:

- the TA identifies the Depositing Service and the Producer Service during operations on the Archives ;

- when an Archive is deposited, the TA is liable to the Customer as soon as he has issued the functional acknowledgement of receipt of the Archive deposited;
- the TA must keep all the documents transmitted by the Client ;
- TA does not do format conversion;
- have sufficient and scalable storage capacity to be able to support the continuous management of records in accordance with contractual commitments;
- comply with the minimum requirements of standard NF Z42-013, in particular the obligations of the TA for the management of documentation (NF Z42-013 chapter 12.1.4 Control of documentation for audits) ;
- allow direct secure access for consultation or extraction of archived information packages;
- respect the application of the access policy to the Archives defined by the Archiving Convention, in particular, take all technical measures to ensure that the archived information packages are accessible only to authorized persons;
- to carry out the destruction of the Archives under the control of the Customer and, after execution, to provide the Customer with the corresponding certificates;
- guarantee the confidentiality of the documents entrusted to him or of which he may have become aware during the contractual relationship with his Client;
- not to analyse and reprocess the documents entrusted by the Customer, except for work explicitly ordered by the Customer (format conversion for example);
- inform the Customer in advance of any technical modifications to be made to its systems and of the consequences on the availability or on the mode of exchange and conservation of the documents entrusted to it;
- in the event that the Archives entrusted to it by the Customer are taken over, to take all measures to guarantee the Customer the return of the entire Archives and all related documents (life cycle logs for example) entrusted to it, guaranteeing their integrity;
- at the end of the contract or in the event of cessation of activity, to be able to fully return the archived information packages and associated elements to the Customer. The TA shall refrain from keeping a copy;
- maintain the quality of the services provided for in the contract and specified in the Services Agreement.

It should be noted that the following commitments are outside the scope of WL e-archiving and this Policy:

- Obtain and maintain the necessary approvals for hosting Public Archives. Nevertheless, the Third Party Archivist may provide an organization wishing to archive Public Archives with the necessary means to obtain the necessary approvals.

6.1.2 The Archiving Authority (AA)

The AA is responsible for the definition of the Archiving Agreement. This defines, among other things, the format of the accepted Archives and the policy for access to the Archives.
In order to specify the technical conditions implemented, the Depositing Service and the Archiving Authority must enter into an agreement (convention, archiving charter, etc.) relating to payments, processing and access to the Archives. This agreement must be fully compliant with the AP.

6.1.3 The Client

The Archiving Service is usually part of a larger Information System. It is the Customer's responsibility to ensure that the Archiving Service corresponds to its needs and regulatory constraints.
The Third Party Archiver provides a set of elements allowing the Customer to facilitate the integration of the Archiving Service in its Information System.

6.1.3.1 Format of the documents

The Third Party Archiver ensures the integrity of the document throughout its life cycle (refer to chapter 3.1.6 this document), and undertakes not to analyze the content of archived documents. Consequently, the Third Party Archiver cannot guarantee the long-term durability of the information content of the document.
The Customer is responsible for the choice of the archiving formats that will be used. However, the Third Party Archiver proposes a set of rules to ensure a better durability:

- The customer is advised to use open formats, i.e. formats whose specifications are easily accessible;
- Formats based on local or international standards may also be considered;
- in the case of a proprietary format, the client must ensure that the format is widely used and that its life span is compatible with the life span of the Archives. Presentation formats as well as print streams are considered proprietary formats ;
- in the case of a tagged format, if it refers to external resources (DTD, XSD, style sheet ...), it is the client's responsibility to archive these resources and to associate them with the archives containing documents in tagged format. When communicating, it is the client's responsibility to retrieve all necessary documents.

The following elements can also help in the choice of target formats:

- limit the use of formats requiring a specific license;
- Ensure that several software solutions are available to access the content of documents;
- verify that an open source software solution allows access to the content of the document ;
- use only stable formats, i.e. without too frequent updates.

When the choice is made to archive digital documents whose format is not known, the management of the sustainability of the documents is the responsibility of the client.

In the event of obsolescence of an archived document format, the Customer is at the initiative of the choice of evolutions of these formats. The Third Party Archiver can accompany the Client in this process.

Presentation formats are not managed by the WL e-archiving service; it is the responsibility of the client to ensure their legibility over time. The Third Party Archiver can accompany the Client in this process.

The Third Party Archiver accepts all document formats, with the reservations expressed above. The list of formats for a given client will be specified in the service agreement.

6.1.3.2 Archiving Policy

For its own use, the Customer or Service Provider must define a record of use of the archive service. This document can be established with the support of the Third Party Archiver, and will describe the elements necessary to understand the integration of the Archiving Service in the Customer's Information System.
It will include:

- a description of the processes involving the Archiving Service;
- a description of the documents to be archived and the associated metadata;
- a filing plan for the Archives;
- a description of the life cycle of each type of Archive;
- an Information Security Policy [ISP] describing the means of securing exchanges;
- a capability plan study.

This document is the sole property of the Customer and should be provided to the Third Party Archiver. The information contained in this document will be necessary for the proper implementation of exchanges and configuration of the service as well as the creation of the Archiving Agreement between the Customer and the Third Party Archiver.

6.1.3.3 Archiving Agreement

The Archiving Agreement is a document describing the use of the Archiving Service by the Customer. It gathers all the information from the Customer's Archiving Policy allowing the Third Party Archiver to set up the service.

6.1.3.4 Deposit

At the time of payment, it is the Customer's responsibility to ensure the quality of the documents provided and the metadata transmitted. It must ensure that its deposits comply with the Archiving Agreement.

6.1.3.5 Verification of Acknowledgements of Receipt

The Customer must check the content of the technical acknowledgement of receipt to ensure that the deposit request has been made, and the functional acknowledgement of receipt to verify that the security of the Archive is complete.
The commitment of the Third Party Archiver is only valid after a positive technical acknowledgement of receipt has been issued when an Archive is deposited.

6.1.3.6 Protection of personal data

In the sense defined by the European Regulation on the protection of personal data [GDPR], the customer is considered to be the data controller and must ensure compliance with the said regulation by the various actors having access to personal data.
The Third Party Archiver may advise the Customer during the implementation of the archiving project. WL e-archiving has interfaces allowing the compliance of documents if personal data is stored and if necessary.

6.1.4 The Producer Service (PS)

The Producer Service designates the entity providing the documents to be archived (documents and metadata). It is outside the scope of this archiving policy.
Responsibilities for securing source documents are borne by the DS, who may, depending on the organization and project context, delegate them to the PS.

6.1.5 The Depositing Service (DS)

The Depository Service refers to the entity that transfers a document to be deposited to an Archiving Authority.
The Depositing Service is responsible for the creation of Archive deposit requests on the Archive Service. It must ensure the validity of the archiving requests and the validity of the results received. The Depositing Service undertakes to provide all information relating to the nature and lifespan of the Archive as well as its possible confidential nature and any restrictions on access to the Archive concerned, where applicable.

The DS can ensure the security of the Archive through the retrieval of the functional attestation.
It is the responsibility of the Depositing Service to check the communicable nature of the Archive or Archive document in accordance with the applicable legislation and regulations (in particular the law of 17 July 1978 as amended and the Heritage Code).
The Depositing Service guarantees that the media and the Archives they contain are in perfect condition and free of any virus or other malfunction likely to have an impact on the proper execution of the Archiving Policy and in particular on the obligations of the Archiving Authority or on the computer means used.

6.1.6 The Control Service

The Controllers are required to carry out their controls in compliance with the laws and regulations governing their powers. If they encounter difficulties in carrying out their controls, they must inform the competent Archiving Authority by any means so that it can take remedial action.

6.1.7 Users

Users must comply with the conditions of consultation and communication relating to the Electronic Archiving Service and the Archive documents processed.
They must also respect the confidentiality, if any, of the Archives documents processed and not attempt to access them if they do not have the associated rights.
Insofar as the User has a specific and personal access method (authentication by login/password), he or she undertakes to keep it confidential and to use it under his or her exclusive control.
Likewise, Users must not attempt to damage all or part of the Secure Electronic Archiving Service and/or its contents.

6.1.8 The operators

The operators are the users of the archiving platform, members of the Third Party Archiver organization whose activities are aimed at the proper functioning of the archiving system.
The roles and responsibilities of the actors are defined in the General Policy [GP] in accordance with the policy defined in the Quality Management System [QMS] of the company.

6.2 Organization of information systems security

The Mediacert Third Party Archiving Committee has an Operational Security Policy for the said service. This policy is compatible with Worldline's [ISP] and extends the [GP] of the TSP. These policies are each maintained and reviewed regularly by their responsible entity.
The Operational Security Policy is a classified document for internal use.
A risk analysis [RA] specific to the Archiving Service has been carried out and is regularly updated. An action plan resulting from the application of the [SOP] and the [RA] is kept up to date and regularly verified by the Mediacert Committee.
The composition and functioning of the Mediacert Committee are defined in the General Policy [GP].
The Archiving Service has a Business Continuity Plan. Refer to chapter 5.1.2 Business Continuity planning of this document.

6.3 Access control

Access to the physical components of the platform is strictly controlled in accordance with the [GP] and [ISP].
The administration of the platform is strictly controlled. Only identified and controlled persons have access to the means of administration of the Platform.

6.4 Journaling

The Archiving Service implements a set of measures in order to concentrate and analyze all the platform's events (see 4.2.2.4).

6.5 Sealing

Sealing is achieved by signing the Archive Description File Mark. This signature is made by means of a private key certified by a recognized certification authority. This sealing is based on the use of a standard format.

6.6 Timestamp

A time countermark is present in the Archive seal. This time countermark comes from a reliable time source.

6.7 Use of rewritable disks

The Archives are stored on magnetic hard disks, which are rewritable disks. This medium complies with current recommendations by using cryptographic means for sealing, encryption and regular verification of the state of the Archive's holdings.