Agfa HealthCare

Global Policy – Information Security & Privacy

Contents

1. Scope

This Global Information Security & Privacy (ISP) Policy is applicable to the Agfa HealthCare global organization irrespective of:

- sites,
- facilities and
- operations.

This policy is applicable to all Agfa HealthCare staff, suppliers, contractors and consultants, irrespective of:

- the nature or duration of their work or
- their geographic location

This policy is applicable to all solutions, products and services, irrespective of:

- the form,
- the technology used,
- the physical location or
- the phase in the lifecycle of the solution, product or service in question.

2. Purpose

This policy expresses the vision of Agfa HealthCare management on Information Security & Privacy.

Important notice – Document convention
Terminology printed in italic are further explained in 9 “Definitions and abbreviations”

3. Context of the organisation

3.1 General context

Agfa Healthcare is a manufacturer of healthcare IT and Radiology products. It is operating in a market with:

- increasingly digitized healthcare and interconnected systems
- more and more regulations and customer requirements

3.2 Interested parties

3.2.1. Internal parties

a) The **Healthcare Executive Committee** (HEC, see section 8) wants to do business with confidence and to be informed about the risks and impacts related to its decisions.
b) The **Sales and Services Organization** needs guidance on:
   - how to integrate ISP in its customer-facing sales and services activities, in an resource-efficient manner (e.g. tenders, contracts, customer requirements).
   - how to deploy, maintain and use products and tools in compliance with ISP regulations and best practices.
c) **Solution Development audiences** need guidance on:
   - how to build products that are in line with ISP regulations and best practices.(e.g. secure coding)

- integrating ISP in their processes (e.g.: data use, supplier management, security testing in development and acceptance)

d) **Agfa Healthcare support functions** like HR and Purchasing need guidance on how to integrate transversal ISP requirements in their processes.

3.2.2. External parties

- **Customers**:
  - will not buy products or services that do not allow them to comply with local regulations.
  - seek transparency from Agfa Healthcare, as part of their supplier due diligence.
  - are not necessarily knowledgeable about ISP.
- **Certification bodies and regulatory authorities**:
  - may audit or inspect Agfa Healthcare's ISP posture, periodically or unannounced.
  - may -depending on their mandate- impose enforcement actions, e.g. withdrawing a certificate, levying a fine, revoking the right to sell in a local market or banning a data processing activity.
- **Patients** are at the heart of most ISP activities, even though Agfa Healthcare rarely interacts with them directly. In today's heightened (media) awareness, patients expect every contributor in the healthcare value chain, to respect their security and privacy.
- **Strategic suppliers**:
  - need to provide services in compliance to Agfa Healthcare ISO27001 certification scope, in particular, the security controls listed in Agfa Healthcare Statement Of Applicability (Node ID: **Document ID:** 28780171 v53.

3.3 *ISMS* Scope and Scope Exclusions

See IMS ID 28781006.

4. Communication

The following communications shall be in place:

What?	When?	With whom	Who?	Why?
Make link to tenders/customer requests visible	Upon request	Customer's account or service manager	ISP Office, bidirectional communi-cation	To answer and meet customer demands
ISP risk moderation, expertise and QA of Solution Development Deliverables	As part of the Solution Development Process	Product Management, Architects, V&V	ISP Office, bidirectional communi-cation	Managing premarket risk
ISP intervention in Complaint, Problem and Defect Management	As part of the After Sales Process	See After Sales subprocesses	ISP Office, bidirectional communi-cation	Managing postmarket risk
Handling internal ISP Incidents and Data Subject Requests	Upon reporting	Initial incident or request contact and relevant organizational stakeholders	ISP Office, bidirectional communi-cation	Containing incidents and managing business and

What?	When?	With whom	Who?	Why?
				regulatory impact
Management reporting	Periodically	• Business Units • HEC • Agfa Group and ICS • GDPR SteerCo	ISP Office, bidirectional communi-cation	Inform stakeholders and business sponsors
Targeted security Training	Periodically or ad hoc	Targeted audiences and general population	ISP Office	Awareness about risks, regulations and best practices
ISP awareness training	Bi-annual	All staff	All of Agfa Healthcare	Best practice & external audit recommendation
Document and record management	In accordance with DRMC procedure	See document and record management and control procedures	All of Agfa Healthcare	Change management.
ISP follow-up per Agfa Healthcare site	Ad hoc	Local Point of Contact	ISP Office	Address local ISP risks and needs
Security consultancy and "evangelism"	Ad hoc	All audiences	ISP Office	Answering questions, taking away concerns

5. Performance evaluation

Performance of the ISMS shall be measured using at least:

- Management review and reporting
- Audits

6. Documents and records management and control

- ISP policies and process documents shall be reviewed at least once every 2 years.
- Records mentioned in this policy shall be documented in the underlying procedures and work instructions.

7. Information Security & Privacy Policy

7.1 Information Security and Privacy Objectives

Agfa HealthCare is committed to support care providers in protecting the privacy of their patients by delivering secure products and services.

We strive:

- to make Information Security & Privacy an integral part of the quality of our products and services and of our organization and operations;

- to protect privacy, especially patient data;
- to comply with privacy and security regulations which are applicable to our organization and customers;
- to secure information as critical asset of our business.

7.2 Obligations

This policy imposes the following obligations:

- securing the Products for our customers;
- securing the Technical and Professional Services for our customers;
- securing the Agfa HealthCare Information & Communication Services;
- securing the Agfa HealthCare core Processes.

7.3 Applicable laws and regulations

Agfa HealthCare shall comply with applicable laws and regulations in the countries and regions where it does business.

7.4 Reference to standards and best practices

In order to implement this policy, Agfa HealthCare has adopted a global risk-based approach to information security in line with the Plan-Do-Check-Act (PDCA) principle.

Agfa HealthCare shall consider the following security & privacy best practices:

- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements;
- ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management;
- ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- ISO/IEC 27799 Health Informatics – Information Security Management in Health using ISO/IEC 27002.
- NIST SP 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- NIST SP 800-172 – Enhancing Security Requirements for Protecting Controlled Unclassified Information

7.5 Policy principles

In order to fulfill our information security objectives as listed in section 7.1, Agfa HealthCare has adopted information security policy principles listed below that correspond to the ISO/IEC 27002 clauses.

7.5.1. Security policy

This policy is the ISP policy of Agfa HealthCare. It is further detailed in global –and when applicable– process documents.

7.5.2. Organization of information security

7.5.2.1. Internal organization

The Agfa HealthCare Executive Committee (HEC), led by the President, is accountable for corporate governance. The management and control of ISP risks is an integral part of this corporate governance.

The HEC gives overall strategic direction by approving and mandating the ISP Policy but delegates tactical responsibilities to the Information Security & Privacy Office, which is led by the *BPO* Information Security and Privacy.

The ISP Office is responsible for the Information Security Management System (ISMS), which is part of Agfa HealthCare's overall Integrated Management System (IMS).

The implementation of ISP process documents falls under the responsibility of the operational units (Business Divisions, Regional Sales & Services Units and Global Support Functions).

To allow for an efficient and coordinated promotion, implementation and integration of this ISP policy, additional roles and responsibilities may be created throughout the organization (see section 8 and 12).

7.5.2.2. Third party management

Agfa HealthCare uses the services of Agfa Global Support Services (GSS), hence Agfa HealthCare's ISP Office shall ensure and monitor that appropriate and agreed information security controls (e.g. through Master Service Agreement (MSA), Service Agreement (SA) and/or Memoranda of Understanding (MoU)) are implemented and maintained.

Agfa HealthCare contractors, consultants, and suppliers shall adhere to and be informed about the ISP policy and process documents. Their employment terms and conditions shall include non-disclosure and confidentiality agreements and/or clauses.

7.5.3. Asset management

An information and information system asset inventory shall be established and maintained. For each asset, or group of assets, a classification identification and ownership shall be defined. Ownership shall be assigned to an individual with sufficient knowledge and authority about the asset and its role in the business processes of Agfa HealthCare.

7.5.4. Human resource security

Specific measurements and guidelines shall be implemented to ensure ISP during the three phases of employment:

- at hiring;
- during employment;
- at termination or change of role and responsibilities.

7.5.4.1. At hiring

Employees shall be informed, upon hiring or change of position within Agfa HealthCare, about their ISP role and responsibilities in their new function. Possible disciplinary action in case of non-compliance with the ISP policy of Agfa HealthCare, shall be communicated. Their employment terms and conditions shall include non-disclosure and confidentiality agreements and/or clauses.

7.5.4.2. During employment

Employees of Agfa HealthCare shall be made aware of their roles and responsibilities w.r.t. ISP. Adequate training and instructions shall be provided.

Especially those employees with access to sensitive information, i.e. *Protected Health Information* (PHI) and *security information,* shall be informed about the private and confidential nature of this data.

Initiatives shall be taken to ensure the establishment and maintenance of ISP awareness throughout Agfa HealthCare.

7.5.4.3. At termination or change of role

When an employee takes up another position within Agfa HealthCare or when she/he leaves Agfa HealthCare, the necessary actions shall be taken to ensure the continued protection of sensitive information.

Special attention is needed in order to remove or modify:

- logical access rights;
- physical access rights;
- roles and responsibilities of the function.

When leaving Agfa HealthCare or when changing positions, assets owned and provisioned by Agfa HealthCare, shall be returned.

7.5.5. Physical and environmental security

Physical access to the sites and offices of Agfa HealthCare and the assets kept in those offices shall be restricted to authorized people only.

Information systems holding unencrypted sensitive information, i.e. PHI and *security information*, shall be located in secure areas. Access to those areas shall only be granted to people with a need-to-know or a need-to-do.

Information and information systems shall be protected against unavailability, loss or damage, e.g. through:

- prevention, detection or protection mechanism in case of:
  - fire,
  - theft or loss,
  - water damage;
- an adequate alternative power supply or other measures to prevent disruption of committed (e.g. through Service Agreements) services.

7.5.6. Communications and operations management

To ensure the correct and secure operation of information systems, process documents shall be established. No evidence is required for aspects which are reasonably expected to be known by employees through their logical or repeated use or deduction.

Special attention shall be given to document processes and/or procedures in the area of:

- day-to-day operational service;
- processing, accessing, exchanging and removing sensitive information i.e. PHI and *security information*;
- staging and configuring systems;
- protection against viruses and malicious code;
- roll-out of new software or updates on customer's infrastructure;
- management of logs and audit trails.

Where possible, segregation of duties shall be established.

7.5.7. Access control

To protect against loss, unauthorized change or misuse of information, access to information and information systems shall be restricted using an identification, authentication and authorization mechanism. Full lifecycle ("joiners, movers, leavers") of identities and their authorization shall be maintained.

Access rights to information and information systems shall be assigned on need-to-know or a need-to-do basis. Unique individual usernames shall be allocated in order to allow for non-repudiation of information handling. Where possible, logging and tracking mechanisms shall be used.

Access to both internal and external networked services shall be controlled and strong authentication shall be used to control access by remote users. Connection to Agfa HealthCare's internal network via public network or dial-in shall be protected appropriately.

As a Cloud service provider, clear guidance on user registration and deregistration functions and specifications for the use of these functions, will be provided to the cloud service customer. (ref ISO 27017- 9.1.1)

7.5.8. Information systems acquisition, development and maintenance

Within Agfa HealthCare two kinds of information systems can be distinguished:

- internal applications: those used to ensure smooth operations of the different business and supporting processes within Agfa HealthCare;
- customer products and services: those information systems which are designed and built for the support of the businesses within the healthcare domain.

Both shall adhere to sound ISP principles.

7.5.8.1. Internal applications

Information security requirements shall be documented in the specifications of new, or to be modified, information systems and applications. These requirements shall be in line with the private

and confidential nature of the processed or stored information and in line with the principles dictated by this document and by regulatory requirements. Special attention shall be given to e.g.:

- access control (authentication and authorization);
- availability of the application and the information;
- logging and auditing capabilities.

Similar considerations shall be made when evaluating a third party's information system and/or application.

Uncontrolled usage of sensitive information i.e. PHI and *security information* is not allowed in the development or test environment. Test data shall be made anonymous where possible.

The principles of access control shall be applied both in the development and test environment.

7.5.8.2. Customer products and services

In order to deliver secure products and services to our customers, ISP measurements or controls shall be included in these products and services as of requirements and design phase. Following ISP controls shall be considered:

- means to protect the confidentiality, integrity and availability of data in transit;
- lock down and hardening principles to minimize security vulnerability exposure;
- availability measurements to ensure that the PHI is available when needed;
- strong access control (authentication and authorization) to PHI based on the least-privilege principle;
- protected audit and logging for the creation, consultation, modification and deletion of PHI.

As a Cloud Service Provider the following policy statements are applicable in alignment with the ISO 27017 5.1.1 controls:

- the baseline information security requirements applicable to the design and implementation of the cloud service;
- risks from authorized insiders;
- single-tenancy and cloud service customer isolation (including virtualization);
- access to cloud service customer assets by staff of the cloud service provider;
- access control procedures, e.g., strong authentication for administrative access to cloud services;
- communications to cloud service customers during change management;
- virtualization security;
- access to and protection of cloud service customer data;
- lifecycle management of cloud service customer accounts;
- communication of breaches and information sharing guidelines to aid investigations and forensics

All processing of PHI/PII should be performed in alignment with the ISO 27018 standard.

As a Cloud Service Provider, AGFA Healthcare will define the allocation of information security incident management responsibilities and procedures between itself and it's cloud service customers. This will include, but not limited to, documentation covering: – the scope of information security incidents that the cloud service provider will report to the cloud service customer; – the level of disclosure of the detection of information security incidents and the associated responses; – the target timeframe in which notifications of information security incidents will occur; – the procedure for the notification of information security incidents; – contact information for the handling of issues relating to information security incidents; – any remedies that can apply if certain information security incidents occur. These activities will be aligned with AGFA HealthCare's' incident management system as defined within it's Integrated Management System.

7.5.9. ISP incident management

ISP is established through the safeguarding of the confidentiality, integrity and availability of information and information systems. Any breach of one of these elements can be a threat to Agfa HealthCare, to the customer or to the patient and is seen as an ISP incident.

An incident management system shall ensure the efficient and effective identification, communication, follow-up and resolving of incidents as well as the decrease or avoidance of (similar) incidents. Where possible logging and tracking mechanisms shall be activated.

Agfa Healthcare employees shall be informed about the nature of ISP incidents and the procedures to report them. They shall report ISP incidents and known or suspected weaknesses as soon as possible.

7.5.10. Business continuity management

Disruption of the core activities, caused by major incidents or disasters, can have a significant economic or reputational impact on Agfa HealthCare.

Special attention shall be given to business continuity threats during risk assessments for solutions.

7.5.11. Compliance

Legal and contractual obligations shall be respected during the development of the ISP policies and process documents.

To ensure compliance with Agfa HealthCare's ISP policy, regular verifications and audits are required. Systems and processes shall be analyzed to ensure they meet the expected ISP levels.

8. Roles and responsibilities

	ACCOUNTABLE
STRATEGIC	President of the HEC HEC Members
TACTICAL **(policy, guide- & baselines)**	Information Security & Privacy Office (led by the BPO ISP)
OPERATIONAL (organization, process, procedures,	Business Division Management (IITS)

work instructions)	Sales & services Organization Manager (Regions) Support Function Manager (MarCom, QARA, Legal, HR, Purchasing, ICS)

Accountable Management may delegate responsibilities but cannot transfer their ultimate accountability. Detailed ISP roles and responsibilities can be found in section 12.

9. Definitions and abbreviations

Term	Description
Protected Health Information (PHI)	*Protected Health Information* (PHI) is any information that relates to the identification of a person (e.g. name, social security number…) and its physical/mental health/condition (images, treatments…) or provision of health care or payment for healthcare.
Security information	*Security Information* is the whole of sensitive security and network settings and of communication, soft- or hardware tools which control access to a system containing PHI or provide means to alter the system's integrity or behavior, e.g.: • passwords, • configuration data, • communication parameters, • security software.
ISMS	Information Security Management System
HEC	Healthcare Executive Committee, the highest management level at Agfa Healthcare.
BPO	Business Process Owner
SaaS	Software as a Service
CSP	Cloud Service Provider
CSC	Cloud Service Customer

Other terms, definitions and abbreviations can be found in the electronic document management system http://intranet.agfa.net/he-ims/ - Glossary http://ims.agfa.net/doc/12462977.

10. References

Process documents that supplement this ISP Policy, can be found in the electronic document management system:
http://intranet.agfa.net/he-ims/support-processes/information-security-privacy/

Name	Doc ID / Location
BPO-BPM Matrix	IMS ID 27295229
ISO/IEC 27001:2013 standard	LL ID 42539638
ISO 27017: 2013 standard	
ISO 27018: 2013 standard	
Section 5.1.1 of the ISO 27002 Code of Practice for Information Security Management	LL ID 42540631
Information Security & Privacy – Roles and Responsibilities	IMS ID 29603632

11. Revision history

For detailed version history and version numbers, refer to Livelink.

Version	Date	Author	Change	Training Requirement?
03	Oct. 2008	G. Claeys	First published version in Livelink	N/A
06	Nov. 2009	Bart Tollebeek	Included organizational ISP structure; differentiated between internal applications and customer product line; lay-out adaptation to template; 3.4.8: clarifications; included 11.6 ISO 27002 classification; review comments Geert Claeys and Steve Abbott.	N/A
08	2010-03-19	Bart Tollebeek	Add Annex 10.1 "Detailed ISP Roles and Responsibilities"	N/A
09	2010-04-19	Bart Tollebeek	Clarification changes to Roles and Responsibilities of Legal after Certification Audit	N/A
12	2012-04-23	Bart Tollebeek	Document review cycle – 1. Removal specific notations of laws and regulations. 2. Replaced Agfa ICS as external party with Agfa Global Support Services. 3. More explicit definition in regards to Access control. 4. BCM defined as risk based dependent. 5. Other changes are mainly to bring wording and definitions in line.	N/A
13	2012-05-21	Bart Tollebeek	Process comments from Livelink Review workflow	N/A
14	2012-06-04	Bart Tollebeek	Editorial change: add link to ISP Roles & Responsibilities in Annex 10.	N/A
15-23	2017-07-10	Wim Hermans, Pierre Kaufmann, Hafiz Anwar	ISO 27002 standard version (year of publishing) removed; typos and format corrected; QARA HSE : HSE removed; Fin&Admin changed to Finance & Controlling; SMCO updated as MarCom; section 5: Links updated / added to IMS homepage, glossary; section 7 : link updated; typos; 3.5.4.3 return of assets rephrased;	No

Version	Date	Author	Change	Training Requirement?
24	2019-12-11	Faysal Boukayoua	Adapted the policy to the most recent organizational changes.	No
25	2021-03-10	Tim Hill	Reduce review cycle from 3 to 2 years to be consistent with QARA review cycle	No
26	2021-10-07	Tim Hill	Document approval workflow	No
27	2021-10-08	Tim Hill	Reviewed as per review cycle.. Added "Strategic suppliers" to Interested Parties. Under Roles & Responsibilities removed Operational Accountability (HCIS, RSD, ICAS, DIIT). Removed mention of "ISP code of conduct" – no such policy document exists.	Yes
28	2021-10-22	Tim Hill	Review – approval rejected – minor typo changes	Yes
29	2021-10-25	Tim Hill	Review - approved	Yes
30	2021-10-27	Tim Hill	Fixed version number	Yes
31	2021-10-27	Tim Hill	On advice from Hafiz S. Anwar (Agfa HealthCare IMS & DRMC Manager) removed requirement for training. ISP training for the whole company is triggered every six months, so ISP training is covered in regular trainings that are pushed to whole company	No
32	2021-11-02	Tim Hill	In section 12.7, replaced "QARA" with "the ISP Office":	No
33	2021-11-16	Tim Hill	In section 7.4 Added references to the NIST standard for protecting controlled unclassified information. In section 7.5.8.2 added a bullet point for lock down and hardening	No

Version	Date	Author	Change	Training Requirement?
34	2023-11-23	Tim Hill	Added cloud specific requirements from ISO27017: 7.4 Added ISO27017 & ISO27018 standards. 7.5.7 Access Control – added ”For SaaS - To manage access to cloud services by a cloud service customer's cloud service users, the cloud service provider should provide user registration and deregistration functions, and specifications for the use of these functions to the cloud service customer ». 7.5.8.2 Customer products and services – added 27017 5.1.1 CSP requirements. 9. Definitions and abbreviations - added SaaS, CSP, CSC 12.5. Owners of information and information systems – added information security incident management responsibilities.	yes
35	2024-03-25	Tim Hill	Republished due to system error	
36	2024-05-06	Jarius Jackson	Updated 7.5.7 and 7.5.8.2. . Added reference links for ISO 27017/IS 27018. Added risk statement to ISP Office Annex. Added statement to ISP Incident Management	

12. Annex: detailed ISP Roles and Responsibilities

Assignment of ISP responsibilities within Agfa Healthcare can be found at IMS ID 29603632.

12.1 Agfa HealthCare Management Committee (HEC)

The HealthCare Management Committee (HEC), led by the President, is ultimately accountable for corporate governance. The management and control of ISP risks is an integral part of this corporate governance.

The HEC gives overall strategic direction by approving and mandating the ISP Policy but delegates tactical responsibilities to the Information Security & Privacy Office, which is led by the BPO Information Security and Privacy.

Its ISP responsibilities shall be at least:

- outline the global ISP policy;
- approve, support, and commit to the ISP global policy;
- provide adequate expertise to implement and maintain an efficient and effective ISP policy;
- conduct regular ISP reviews;
- review and discuss critical or non-acceptable ISP incidents, -problems or risks.

12.2 ISP Office

The ISP Office is responsible for the tactical ISP responsibilities. These shall be at least:

- develop strategic ISP policy, global guide- & baselines and work instructions;
- ensure ISP training is developed and maintained;
- monitor and assess the status of the ISP policy and ISP incidents within Agfa Healthcare;
- manage – in close cooperation with QARA – the ISP Risk Management process;
- classifying risks of information systems and assets; minimally based on the CIA Triad but expandable based upon industry best practices and as deemed beneficial in alignment with business goals and objectives;
- where needed escalate critical risks into the Corrective And Preventive Action (CAPA) process;
- report the status of the ISP policy and ISP incidents to the ISP Council and HEC;
- define and safeguard the ISP requirements in the Master Service Agreement (MSA), Service Agreement (SA) and/or Memoranda of Understanding (MoU) with Agfa GSS for the delivery and support of services to Agfa HealthCare;

12.3 BU, BD and SSU responsibilities

The Business Divisions (BDs), Business Units (BUs) and Sales & Service Units (SSUs) are responsible for implementing ISP controls.

They shall have at least the following responsibilities:

- design, review and adjust the global ISP policy and process documents and their implementation;

- review and discuss ISP incidents and -problems and propose solutions to the HEC when critical ISP incidents, problems or risks occur;
- review and adopt in the ISP policy any relevant changes in healthcare laws and regulations;
- formalize the ownership of global information and information systems.

12.4 Management of BD/BU and SSU

Management is accountable for day-to-day ISP activities and for compliance within his/her area of authority.

BD/BU/SSU management shall have at least the following responsibilities:

- address/communicate the ISP policy and process documents prior to and during employment, to subordinates;
- coordinate and monitor ISP training for his/her employees;
- ensure implementation of and compliance with the ISP policy, its global minimum baseline requirements and process documents;
- implement the ISP process documents in the SSU, BU or BD;
- communicate the creation, modification or removal of access rights of an employee via the proper channel (e.g. UAT).

12.5 Owners of information and information systems

Owners are accountable for the ISP of the information and/or information systems they manage.

Their responsibilities shall be at least:

- classify the information and information systems;
- apply the ISP policy and process documents to their day-to-day activities;
- cooperate with the planning, development and execution of the business continuity planning;
- plan and develop acceptance tests for applications;
- approve or deny access to confidential information;

12.6 Employees

Employees shall make ISP an integral part of the quality of Agfa HealthCare's products and services and of the organization and operations. They shall learn and adopt ISP in their professional activities.

Agfa Healthcare employees shall have at least the following responsibilities:

- become familiar with ISP policies and process documents that are relevant for their role;
- comply and commit to the ISP policy and process documents when performing day-to-day activities;
- safeguard ISP in day-to-day activities;
- report ISP incidents or weaknesses to the ICS Service Desk;
- attend ISP awareness initiatives, e.g. Agfa Learning Management System (LMS) modules;
- cooperate with (internal or external) ISP audits.

12.7 Quality Assurance, Regulatory Affairs

The ISMS is incorporated in the Integrated Management or Quality System (IMS). The ISMS needs shall be addressed in the IMS and its processes.

To ensure that the selected ISP controls have been implemented and maintained in Agfa HealthCare's processes, applications and information systems and to maintain the ISO 27001 certification, recurrent audits are planned and executed by QARA.

The responsibilities of the internal auditor shall be at least:

- gain knowledge of the ISP policy and process documents and about the selected ISO 27002 controls;
- develop and follow-up the audit plan;
- report any non-conformities, deficiencies, observations and/or recommendations to the HEC;
- inform any non-conformities, deficiencies, observations and/or recommendations to stakeholders that should follow up or that are impacted;

As business and regulatory requirements continuously evolve, Agfa HealthCare shall ensure that the risks its business is facing are treated appropriately. Therefore recurrent ISP risk assessments are conducted by the ISP Office

The responsibilities of the ISP Risk manager shall be at least:

- coordinate ISP risk assessments;
- participate in the risk assessment;
- report on the status and the ISP level to stakeholders that should follow up or that are impacted;
- recommend possible risk treatment improvements.

12.8 Legal

To comply with privacy and security legislations that are applicable to Agfa HealthCare, its customers or its suppliers, local legislative requirements shall be monitored and where needed incorporated in Agfa HealthCare's processes.

The Legal Team's responsibilities shall be at least:

- identify, maintain and communicate ISP legislations;
- provide feedback to questions w.r.t.:
  - ISP questions in third-party agreements;
  - local healthcare and cryptography legislations.

12.9 Human Resources

To ensure that all employees are informed about and understand ISP, Human Resources (HR) shall assist line management with the implementation of specific ISP measurements and guidelines.

HR shall be responsible at least for:

- addressing ISP prior, during and after employment;
- addressing ISP in the terms and conditions of employment;

- organizing ISP awareness and training for all employees;

12.10 Agfa GSS

Agfa GSS are responsible for providing services to Agfa HealthCare satisfying Agfa HealthCare's ISP requirements, as covered by Master Service Agreements (MSA), Service Agreements (SA) and/or Memoranda of Understanding (MoU).

12.11 Third Parties

Some third-parties (i.e. suppliers) play an vital role in the support and maintenance of Agfa HealthCare's commercial products. Therefore they shall adhere to the ISP policy as set forth by Agfa HealthCare.

Third parties shall be responsible at least for:

- adhere to the ISP requirements as per third party agreements.

AGFA

Details as of PDF Creation Date

Document Metadata

Title:	Global Policy - Information Security and Privacy
Livelink ID:	26326336
Version#:	37
Version Date:	2024-05-07 04:17 AM CET
Status:	Approved on 2024-05-07 03:43 PM CET
Owner:	Hafiz Anwar (axnru)
Created By:	Peter Guldentops (amlpo (Delete) 7798405)
Created Date:	2008-10-07 11:58 AM CET
PDF Creation Date:	2024-05-07 03:43 PM CET

This document was approved by:

Signatures:

1. Tim HILL (epncm) on 2024-05-07 03:05 PM CET

Detailed Approver History:

- **Approval Workflow started on 2024-05-07 03:04 PM CET**
  - Approval task originally assigned to and completed by Tim HILL (epncm) on 2024-05-07 03:05 PM CET

Version & Status History

Version#	Date Created	Status
37	2024-05-07 04:17 AM CET	Approved - 2024-05-07 Reviewed - 2024-05-07
36	2024-05-07 04:16 AM CET	
35	2023-11-27 10:46 AM CET	Published - 2024-03-26 Published - 2024-03-26 Unpublished - 2024-03-25 Published - 2023-12-06 Published - 2023-12-06 Published - 2023-12-06 Approved - 2023-12-06 Reviewed - 2023-11-28
34	2023-03-16 04:27 AM CET	Reviewed - 2023-04-19
33	2021-11-16 02:37 PM CET	Unpublished - 2023-12-06 Review Cancelled - 2023-03-16 Published - 2022-03-28

		Published - 2022-03-28 Approved - 2021-11-22
32	2021-11-02 02:04 PM CET	Unpublished - 2022-03-28 Published - 2021-11-10 Published - 2021-11-10 Published - 2021-11-10 Published - 2021-11-10 Published - 2021-11-10 Unpublished - 2021-11-10 Approved - 2021-11-05
31	2021-10-27 08:22 AM CET	Approval Cancelled - 2021-11-02
30	2021-10-27 08:14 AM CET	
29	2021-10-22 11:10 AM CET	Approved - 2021-10-25
28	2021-10-22 09:17 AM CET	Rejected - 2021-10-22

Applied Categories and Attributes:

IMS	
Effective Date:	12/06/2023
Review Date:	12/01/2025
IMS Editor:	Hafiz Anwar (axnru)
Document Owner:	Tim HILL (epncm)
Doc Type:	Policy
Org Level:	Global HealthCare -> Global HealthCare
Process:	Information Security & Privacy -> Information Security & Privacy
Site:	All
Global Process Roll Out:	N/A
ITCo Library	
Document Type:	User Manual
Category > SubCategory > Item:	Tools & Processes > General Info > General Info
Content Manager:	Tim HILL (epncm)
Summary:	
Language:	English
Availability:	Internet
Language Master Document:	
Software Download URL:	
IMS HE	
Effective Date:	12/06/2023
Review Date:	12/01/2025
IMS Editor:	Hafiz Anwar (axnru)
Document Owner:	Tim HILL (epncm)
Doc Type:	Policy
Org Level:	Agfa HealthCare -> Agfa HealthCare

Process:	Information Security & Privacy -> Information Security & Privacy
Site:	All
Global Process Roll Out:	N/A

Applied Classifications:

Published -> QMS -> Document Type -> Policy
Published -> QMS -> Subsystem of QMS -> Management responsibility
Published -> QMS -> Department -> All departments
Published -> QMS -> Organization Level -> All Organizational levels