1 Objective

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

The policy creates a framework for Agfa to protect through its operations and processes, within reason, all information in scope from any threats, whether internal, external, deliberate or accidental and to mitigate remaining risks towards an acceptable level.

2 Scope

This global Information Security & Privacy (ISP) policy is applicable to all organizations belonging to the Agfa Group and those organizations affiliated with the Agfa Group and to which Agfa policies apply irrespective of:

- Site
- Facilities and
- Operations

In the remainder of the text, Agfa refers to all the above organizations.

This policy covers information and data (hereinafter referred to as "Data") that Agfa handles in its activities, solutions, products and services during their entire lifecycle, as manufacturer, service provider, data controller or data processor.

Information takes many forms and includes information stored on computers and various other intelligent devices (such as smart phones, tablets, ...), transmitted across networks, printed out or written on paper, sent by fax, stored on tape, disk or usb stick, or spoken in conversation and over the phone.

By handling is meant, without being exhaustive, any operation or set of operations (which is performed on Information) whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, irrespective of the media, engines and platforms being used.

This policy applies to all Agfa staff and to all Agfa sites, suppliers, contractors and consultants, irrespective of:

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

3 Table of content:

4 Information Security & Privacy Policy

4.1 Information Security and Privacy Objectives

Agfa is committed to being an organization that secures information and protects privacy of that information, irrespective of whether it is owned by (as data controller) or entrusted to *Agfa (as data processor).*

As such, *Agfa* strives:

- to make information security & privacy an integral part of the quality of *Agfa* solutions, products and services and of its organization and operations;
- to secure information as critical assets of the *Agfa* business
- to protect information of partners and customers
- to respect privacy, particularly of employees, partners and customers
- to comply with various privacy and security regulations which are applicable to *Agfa* and its various activities
- to create a corresponding awareness, insight and knowledge with *Agfa* employees

4.2 Obligations

This policy imposes the following obligations:

- information is protected against unauthorized access;
- confidentiality of information is assured;
- integrity of information is maintained;
- business requirements for the availability of information and information systems are met;
- products and services are secured for our customers
- securing Agfa core processes
- information is stored only as long as necessary for the fulfillment of the purposes for which it was collected;
- information will be released to law enforcement upon receipt of a valid judicial instruction;
- compliance with regulatory and legislative requirements is met;
- business damage is minimized by preventing or minimizing the impact of security incidents

4.3 Applicable laws and regulations

Agfa will comply applicable laws and regulations in the countries and regions where it does business.

4.4 Standards

In order to implement this policy *Agfa* has adopted a global risk based approach to information security in line with the Plan-Do-Check-Act (PDCA) principle. *Agfa* will take into account the following standard:

- ISO/IEC 27001:2013 Information technology – security techniques – information security management systems – requirements;
- ISO/IEC 27002:2013 Information technology – security techniques – code of practice for information security management;

And where applicable:

- ISO/IEC 27799 Health Informatics – information security management in Health using ISO/IEC 27002.

4.5 Policy principles

In order to implement our information security objectives as listed in 4.1, Agfa has adopted information security policy principles listed below that correspond to the ISO/IEC 27002 clauses.

4.5.1.1 Security policy

This policy is the ISP policy of Agfa. It is further detailed in global and / or local guidelines and when applicable, process documents.

4.5.2 Organization of information security

4.5.2.1 – Internal Organization

Within *Agfa* the Executive Management Meeting (EMM), led by the CEO, is upon delegation by the Board of Directors accountable for corporate governance as a whole. The management and control of ISP risks is an integral part of this corporate governance.

The EMM gives overall strategic direction by approving the ISP principles but delegates tactical responsibilities for ISP to the Agfa Information Security Council (ISC), led by the CFO.

The Agfa Information Security Officer is responsible for the Agfa Information Security & Privacy Policy of Agfa and the Tactical coordination of Information Security at Agfa.

The Leadership team of a Business Group, led by the President, is accountable for corporate governance as it relates to that Business Group. Management and control of ISP risks relating to that Business Group is an integral part of their corporate governance.

The Leadership team of a Business Group gives 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 or the Security Officer for the Business Group.

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

The implementation of ISP process documents is under the authority of the operational units (Business Divisions, Sales & Services Organizations and Global Support Functions).

The Agfa Information Security Officer has responsibilities for maintaining the policy and providing advice and guidance on its implementation.

Accountable Management may delegate responsibilities for duties and tasks, but cannot transfer their accountability that the required duties and tasks are executed.

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 5).

4.5.2.2 Third party management

Agfa Business Groups use the services of Agfa Global Support Services (GSS), hence they 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 contractors and consultants 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.

4.5.2.3 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.

4.5.2.4 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.

4.5.2.4.1 At hiring

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

4.5.2.4.2 During employment

Employees of Agfa shall be made aware of their roles and responsibilities with respect to ISP. Adequate training and instructions shall be provided.

Especially those employees with access to sensitive information, i.e. *Protected Health Information* (PHI), Personally Identifiable Information (PII) 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.

4.5.2.4.3 At termination or change of role

When an employee takes up another position within Agfa or when she/he leaves Agfa, they shall be informed about their ISP role and responsibilities in their new function and 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 or when changing positions, assets owned and provisioned by Agfa, shall be returned.

4.5.2.5 Physical and environmental security

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

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

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.

4.5.2.6 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, PII 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.

4.5.2.7 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 internal network via public network or dial-in shall be protected appropriately.

4.5.2.8 Information systems acquisition, development and maintenance

Within Agfa three kinds of information systems can be distinguished:

- internal IT systems: those used to ensure smooth operations of the different business and supporting processes within Agfa;
- internal Operational Technology (OT) systems: hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events
- customer products and services: those information systems which are designed and built for the support of the businesses within the Business Group domain.

All will adhere to sound ISP principles.

4.5.2.8.1 Internal systems

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;
- protection of PHI, PII and security information;

Similar considerations shall be made when evaluating a third party's information system and/or application. Uncontrolled usage of *Sensitive 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.

4.5.2.8.2 Operational Technology systems

In order to ensure continued operation of processing facilities, ISP measurements or controls shall be included in these systems as of the requirements and design phase. Following ISP controls shall be considered:

- means to protect the confidentiality, integrity and availability of data in transit;
- access control (authentication and authorization), including 3rd party access;
- risk of impacting none OT systems through Cyber incidents;
- logging and auditing capabilities.

4.5.2.8.3 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;
- availability measurements to ensure that the PHI, PII and customer data is available when needed;
- strong access control (authentication and authorization) to customer data, including PHI, based on the least-privilege principle;
- protected audit and logging for the creation, consultation, modification and deletion of customer data, including PHI and PII.

4.5.2.9 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, to the customer or to the customer's customer 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 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.

4.5.2.10 Business continuity management

Disruption of the core activities, caused by major incidents or disasters, can have a significant economic or reputational impact on Agfa. Special attention shall be given to business continuity threats during risk assessments for internal applications as well as customer products and services.

4.5.2.11 Compliance

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

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

5 Roles and responsibilities

	ACCOUNTABLE
STRATEGIC	CEO EMM Members (Delegated to ISC)
TACTICAL **(policy, guide- & baselines)**	Agfa Information Security Council (Led by CFO) Agfa Information Security Officer
OPERATIONAL (organization, process, procedures, work instructions)	Business Division Management (HealthCare, Radiology Solutions, Offset, DPC) Support Function Manager (Finance, Innovation Office, MarCom, QARA, Legal, HR, Purchasing, ICS, Supply Chain/Logistics, Legal, Materials Manufacturing, Program Office)

Accountable Management may delegate responsibilities but cannot transfer their ultimate accountability.

6 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.
Personally Identifiable Information (PII)	*Personally identifiable information* (PII) is information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.
Sensitive Information	*Sensitive Information* is information that covers the three main areas of PHI, PII and Security Information plus Customer and Agfa data that is of high Intellectual Property value.
Security information	*Security Information* is the whole of sensitive security and network settings and of communication, software or hardware tools which control access to a system containing sensitive information 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
EMM	Executive Management Meeting, the highest management level at Agfa.
BPO	Business Process Owner

7 Policy Review

This policy is reviewed at least every three years or sooner, whenever internal or external changes require an adaptation of this policy.