


Company:		Title:				
		Information Security Management System Policy				
Document						
Code:	AMR-ADM-ISMS-POL01	Revision :	1.07	Date:	16.09.2023	Pag.1/4

Made by: Adrian Serghei
SA

Verified: Dobre Mihaela
CISO

Approved: Cristian Moldovan
Director General

Date: 16.09.2023

Copy: x controlled ☐ uncontrolled Copy nr. 1


Information Security Management System Policy

Revision history:

16.09.2023	1.07	Adrian Serghei	Publish the 7th version of the document
11.05.2022	1.06	Adrian Serghei	Publish the sixth version of the document
12.06.2021	1.05	Adrian Serghei	Publish the fifth version of the document
24.06.2020	1.04	Adrian Serghei	Publish the fourth version of the document
27.02.2020	1.03	Adrian Serghei	Publish the third version of the document
08.08.2019	1.02	Adrian Serghei	Publish the second version of the document
19.04.2019	1.01	Adrian Serghei	Publish the first version of the document
Date	Version	Author	Comments

Distribution List:

Nr. crt.	Name and surname	Function	Type	Date when received
1	All Departments		electronic	19.04.2019
2	All Departments		electronic	08.08.2019
3	All Departments		electronic	07.02.2020
4	All Departments		electronic	24.06.2020
5	All Departments		electronic	12.06.2021
6	All Departments		electronic	11.05.2022

Company:		Title:				
		Information Security Management System Policy				
Document						
Code:	AMR-ADM-ISMS-POL01	Revision :	1.07	Date:	16.09.2023	Pag.1/4

7	All Departments		electronic	16.09.2023
---	-----------------	--	------------	------------

Introduction

In accordance with the provisions of this document, Information and Communication Resources (RIC) provided and administered by Ameropa Grains SA are considered strategic assets of the company and should be managed accordingly.

The field of activity of **Ameropa Grains SA** is *distribution of fertilizers for agriculture, seeds, and pesticide in Romania*.

Compromising the security of these resources may affect the company's ability to provide information and communication services, may lead to fraud or destruction of data, in violation of contractual terms, disclosure of commercial trade secrets, damage to the credibility and reputation of the company and legal liability.

This policy is set:


- To be in accordance with the statute, regulations, laws and other official documents in force on public information resource management such as:
 - LAW no. 182 of 12 th April 2002 on the protection of classified information
 - GOVERNMENT DECISION no. 585/2002 - The National Standards on the Protection of Classified Information in Romania
 - GOVERNMENT DECISION no. 353/2002 on Norms on the Protection of NATO Classified Information in Romania
 - GOVERNMENT DECISION no. 781 / 25 th July 2002 on the protection of restricted information
 - Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data
 - The General Data Protection Regulation (EU) 2016/679 ("GDPR")
 - LAW no.506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector
 - Order No. 52/2002 on approving the minimum safety requirements for personal data processing
 - Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law
- To establish prudent and acceptable practices regarding the use of Ameropa Grains' RIC.
- To train users who are entitled to use the RIC on the responsibilities associated with such use.

Audience

Ameropa Grains ISMS policy applies equally to all Ameropa Grains SA personnel that are allowed access to Ameropa's computing and communications resources.

The following entities and users are covered separately by the provisions of the Policy:

- Employees with fixed-term employment contract or indefinite period having access to information and communication system;

Company:		Title:				
		Information Security Management System Policy				
Document						
Code:	AMR-ADM-ISMS-POL01	Revision :	1.07	Date:	16.09.2023	Pag.1/4

- The 3rd parties (collaborators or suppliers), who have access to Ameropa Grains' RIC;
- Other persons, entities or organizations, interested parties that have access to Ameropa Grains' RIC.

Purpose

The ISMS policy is aimed to ensure the integrity, confidentiality and availability of information.


- Confidentiality refers to the protection of data against unauthorized access.
- Electronic files created which are sent, received or stored using the system's own RIC, managed or under the custody and control of Ameropa Grains SA may be categorized as confidential and can be accessed only by authorized personnel.
- Integrity refers to the measures and procedures used to protect data against unauthorized modifications or destruction.
- The availability ensures the continuous operation of all components of the RIC. Different applications require different levels of availability depending on the impact or damage as a result of RIC not working properly.
- The security policy aims also to establish the necessary framework for the development of regulations and safety procedures. These are mandatory for all users RIC.

Objectives

ISMS is intended to protect information to an appropriate extent by maintaining the level of risks to the organization at an acceptable level.

Effective ISMS enables information to be used and shared while protecting its value. In this way, our organization can maintain efficient operations, achieve legal compliance/contractual or other requirements and maintain its reputation.


Our organization will have its way of dealing with information risk and will take this into account when deciding what controls to implement. All users are responsible for contributing to Ameropa Grains' RIC: their actions, or inaction, can protect or expose information to risk.

Company:		Title:				
		Information Security Management System Policy				
Document						
Code:	AMR-ADM-ISMS-POL01	Revision :	1.07	Date:	16.09.2023	Pag.1/4


Objectives 2020-2023:

ISO Annex A Domain #	ISO 27001:2013 Annex A Domain	Metrics Short Name	Objective of Metrics	Metrics	Positive / Negative Metrics	Frequency	Target	Measure	Task	Responsible Function	Source of Data	Implementation term	Status
10	Cryptography	QES implementation	Facilitate teleworking and reduce amount of printed documents	% of all employees	Increasing is better	Yearly	95%	Percentage	Assign an e-signature and create a remote signing account	CISO/System Administrators	E-signature Deployment status	31.12.2020	100%
6	Teleworking	Teleworking	Improve teleworking preparedness	% of main office employees (with computer access) with laptops	Increasing is better	Yearly	100%	Percentage	Issue a laptop to every main office employee with computer access	System Administrators	AMR-IT-ISMS-FORM22 - ASSET REGISTRY	31.12.2020	100%
12	Backup	Local files backup	Backup files on local computers	% of Office 365 E3 users with OneDrive backup	Increasing is better	Yearly	100%	Percentage	Setup OneDrive for file backup on local computers	System Administrators	User admin center	31.12.2020	100%
16	Information Security Incident Management	Security incidents	Keep the number of security incidents which result in exposure of personal information and the need to inform authorities to zero %	% of total security incidents	Decreasing is better	Yearly	0%	Percentage	Use appropriate controls to manage security risks	System Administrators	Incident and Actions Register.	31.12.2020	100%

ISO Annex A Domain #	ISO 27001:2013 Annex A Domain	Metrics Short Name	Objective of Metrics	Metrics	Positive / Negative Metrics	Frequency	Target	Measure	Task	Responsible Function	Source of Data	Implementation term	Status
1	Access to networks and network services	Enable MFA	Enable MFA for all main office users with Office 365 E3 license	% of all employees with Office 365 E3 license from main office	Increasing is better	Yearly	100%	Percentage	Enable MFA for all main office users	System Administrators	Office 365 admin portal	31.12.2021	98%
2	Controls against malware	Computers with virus/malware infections	Keep the number of computers with virus/malware infections under 5%	% of computers infected with virus/malware from app protected computers	Decreasing is better	Yearly	<5%	Percentage	Monitor and reduce number of infected computers	System Administrators	TrendMicro Portal	31.12.2021	3%
3	Teleworking	Teleworking	Improve teleworking conditions	% of main office employees using VPN	Increasing is better	Yearly	100%	Percentage	Install AO-VPN as a teleworking solution for users	System Administrators	VPN Server Logs	31.12.2021	100%

Company:		Title:				
		Information Security Management System Policy				
Document						
Code:	AMR-ADM-ISMS-POL01	Revision :	1.07	Date:	16.09.2023	Pag.1/4

ISO Annex A Domain #	ISO 27001:2013 Annex A Domain	Metrics Short Name	Objective of Metrics	Metrics	Positive / Negative Metrics	Frequency	Target	Measure	Task	Responsible Function	Source of Data	Implementation term	Status
11	Equipment siting and protection	Bitlocker implementation percentage	Enable disk encryption on all computers with TPM	% of HQ computers with TPM	Increasing is better	Yearly	100%	Percentage	Enable disk encryption using Bitlocker	System Administrators	AD Bitlocker Management	31.12.2022	100%
ISO Annex A Domain #	ISO 27001:2013 Annex A Domain	Metrics Short Name	Objective of Metrics	Metrics	Positive / Negative Metrics	Frequency	Target	Measure	Task	Responsible Function	Source of Data	Implementation term	Status
12	Operations Security	Number of computers with domain policy applied	To identify the number of systems in use joined in ameropa.dom domain and having domain policy applied	Number of active computers with domain policy applied x 100/Total number of computers in use	Increasing is better	Yearly	100%	Percentage	Join computers to amerooa.dom domain	System Administrators	Asset registry	31.12.2023	81%

Company:		Title:				
		Information Security Management System Policy				
Document						
Code:	AMR-ADM-ISMS-POL01	Revision :	1.07	Date:	16.09.2023	Pag.1/4

In conducting specific activities, the followings will be applicable:

- compliance with applicable legal and regulatory requirements and contractual obligations regarding information security;
- identification, analysis, evaluation, communication and treatment of information security risks/opportunities, annually or whenever necessary;
- establishing, updating and communication system rules and working on information security;
- controlled access to the building, facilities, assets, networks, documents, files and media;
- monitoring and recording company's interested parties and access to RIC;
- monitoring and recording the remote access to files and servers of the Organization;
- signaling and processing security incidents and deficiencies, application security measures prompt and effective action analysis;
- develop plans and response capacity in emergency situations;
- continual improvement of the Information Security Management System.

For the application of its ISMS, Ameropa Grains' CEO named CISO (Chief Information Security Officer) as responsible for operational management and maintenance of the ISMS.

All employees, contractors, 3rd parties or interested parties who have access to Ameropa Grains' RIC have a duty to comply with this established policy and safety procedures/policies and to report all suspected incidents of actual or by CISO.

In applying this policy are established safety procedures.

This policy is available for all Ameropa Grains SA employees and interested parties, on demand and on the website.