

**DECISION OF THE AGENCY FOR THE COOPERATION OF ENERGY
REGULATORS No 01/2015**

of 10 February 2015

REMIT INFORMATION SECURITY POLICY

THE AGENCY FOR THE COOPERATION OF ENERGY REGULATORS,

HAVING REGARD to Regulation (EC) No 713/2009 of the European Parliament and of the Council of 13 July 2009 establishing an Agency for the Cooperation of Energy Regulators¹,

HAVING REGARD to Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency² (REMIT), in particular Article 12(1), first and third subparagraph, thereof,

HAVING REGARD to the Commission Implementing Regulation (EU) No 1348/2014 of 17 December 2014 on data reporting implementing Article 8(2) and Article 8(6) of Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency³,

WHEREAS:

- (1) The Agency should ensure the operational reliability, confidentiality, integrity and protection of the information received pursuant to Article 4(2) and Articles 8 and 10 of REMIT and take all necessary measures to prevent any misuse of, and unauthorised access to, the information maintained in its systems.
- (2) The Agency should identify sources of operational risk and minimise them through the development of appropriate systems, controls and procedures.
- (3) It is appropriate to establish operational procedures and measures to ensure that all activities which require handling of information collected under REMIT obligations are covered by a comprehensive security system for protecting it.
- (4) The Agency has implemented its REMIT Information System (ARIS) and the Information system for management and/or sharing of REMIT Case information to meet REMIT obligations on wholesale energy market data collection, market monitoring and data sharing.

¹ OJ L 211, 14.8.2009, p.1.

² OJ L 326, 8.12.2011, p.1.

³ OJ L363, 18.12.2014, p.121.

- (5) It is necessary for the Agency to ensure the confidentiality, integrity and availability of ARIS information and assets against threats, whether internal or external, deliberate or accidental.
- (6) The security of REMIT information is vital to prevent market abuse and to foster open and fair competition in wholesale energy markets for the benefit of final consumers of energy.
- (7) The operational security of the IT systems used for processing and transmitting the data is key to the achievement of the level of protection requested by REMIT for the handling of collected data.
- (8) It is appropriate that, to this end, the Agency works closely with the European Network and Information Security Agency (ENISA) in setting up an IT system that ensures the highest possible level of data confidentiality.
- (9) It is therefore necessary to implement these principles and requirements through the REMIT Information Security Policy of the Agency.
- (10) The Agency should determine the appropriate framework for sharing relevant information held by the Agency with other Union institutions, bodies, offices or agencies, as appropriate, in accordance with this Decision and inter-institutional arrangements in force.
- (11) The Agency should give access to the mechanisms to share information it receives in accordance with Articles 7(1) and 8 of REMIT only to authorities which have set up systems enabling the Agency to meet the requirements of Article 12(1) of REMIT and which ensure the confidentiality, integrity and protection of information which they receive pursuant to Articles 4(2), 7(2), 8(5) or 10 of REMIT and take steps to prevent misuse of such information.
- (12) In order to ensure the application of the security rules for protecting REMIT information through ARIS following the entry into force of Commission Implementing Regulation (EU) No 1348/2014 and the Agency's need to launch ARIS applications in a timely manner, this Decision should enter into force on the date of its signature. The EU classification of REMIT information can currently be left undecided and be subject to a separate Decision.
- (13) The Agency is in the course of adopting its Security Policy. Once it is formally adopted, the Agency's REMIT Information Security Policy shall be an integral part of the Agency's Security Policy,

HAS ADOPTED THIS DECISION:

Article 1

The Agency's REMIT Information Security Policy, as annexed to this Decision, as per Annex I and II, is hereby adopted.

The EU classification of REMIT information in the Agency's REMIT Information Security Policy is suspended and will be subject to a separate Decision on the EU classification of REMIT information.

Article 2

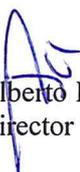
1. The Head of the Market Monitoring Department is mandated to adopt measures of management and administration to assign roles and responsibilities, to implement and operate the policy and to ensure compliance with the policy in the Market Monitoring Department in order to implement this Decision.
2. The measures identified in the first paragraph of this article shall be communicated to the Director prior to their adoption.

Article 3

This Decision shall enter into force on the date of its signature. This Decision shall be communicated to the staff, brought to the attention of the Staff Committee and published on the intranet of the Agency.

Done at Ljubljana on 10 February 2015.

For the Agency:


Alberto Pototschnig
Director

ANNEX I: The Agency's REMIT Information Security Policy

Introduction

The Agency has implemented its REMIT Information System (ARIS) to meet REMIT obligations on wholesale energy market data collection, market monitoring and data sharing.

According to the requirements set out in Article 12 of REMIT, ARIS must be operationally reliable. In particular, the Agency shall take all the necessary measures to prevent any misuse of, and unauthorised access to, the information maintained in ARIS.

The concept of data sharing as foreseen in REMIT creates a risk to the security of information as it is intended that copies of parts of the information are shared among institutions in the EU 28 Member States. Therefore, the strategy to secure information designed in these policies can only mitigate the risk, but the general problem will remain, that copying information and sharing it creates own risks to the security of the information and to the information itself.

This Information Security Policy addresses REMIT information in any form and specifies adequate protection to the extent required by REMIT and its implementing acts.

Numerous entities, agencies and authorities share REMIT information (see Figure 1 – Organisations originating and sharing REMIT information), boundary of information sharing is the blue rectangle.

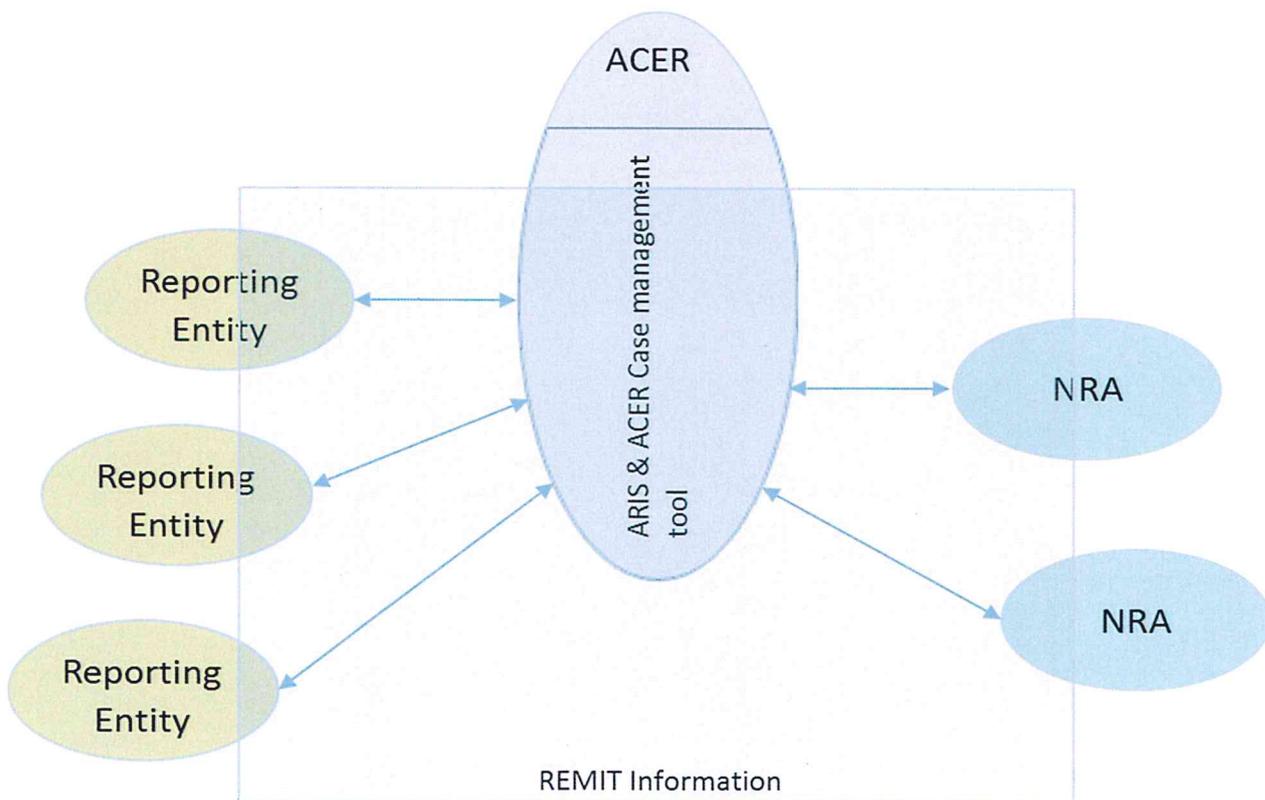


Figure 1 – Organisations originating and sharing REMIT information

This information security policy is aimed to ensure:

- Confidentiality
- Integrity, and
- Availability

of REMIT information and underlying assets against threats, whether internal or external, deliberate or accidental.

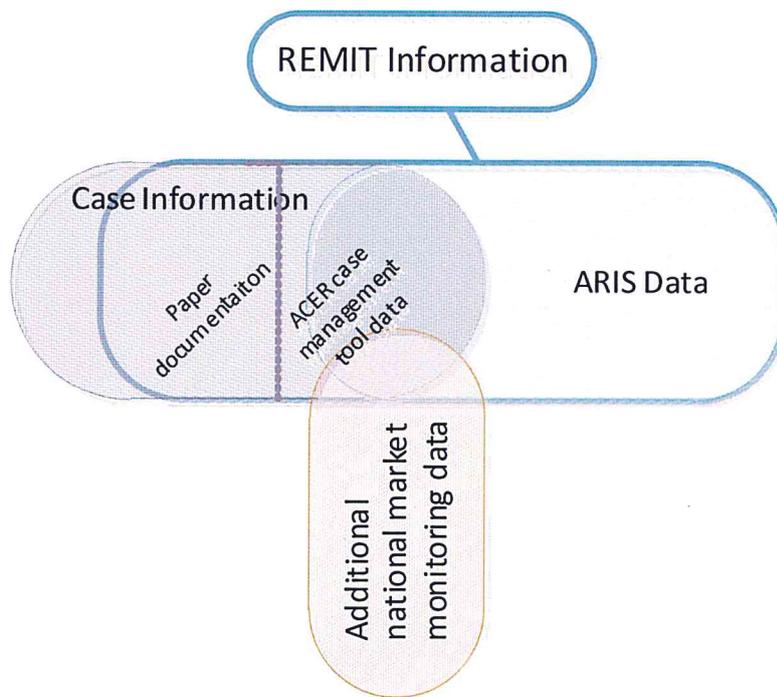


Figure 2 - REMIT information

Please refer to the chapter Definition of terms for a detailed description of various data groups represented in **Figure 2 - REMIT information**.

Policy Scope

All processes, activities and assets implemented to enable the Agency to fulfil REMIT framework responsibilities are within the scope of this information security policy, especially:

1. Market surveillance and analysis;
2. Case handling;
3. Case support;
4. Reporting;
5. ARIS and CASE management tool governance and management;

6. Data and information exchange procedures and interfaces with persons and authorities that should provide the Agency with information and data about wholesale energy market transactions (as stated in Articles 4(2) and 8 of REMIT);
7. Data and information exchange procedures and interfaces with national regulatory authorities, competent financial authorities of the Member States, national competition authorities, ESMA and other relevant authorities (as stated in Article 10(1) of REMIT);
8. All communication channels used for communication and transfer of information and data related to points 1. to 5. of this list.

From the information and information sharing perspective, the scope of this policy includes REMIT information.

Not in scope of this policy is:

- Additional national market monitoring data
- Case information that is not REMIT case information

The scope of this policy is schematically represented in **Figure 1 – Organisations originating and sharing REMIT information** as blue rectangle.

Policy Applicability

Basic principles and requirements laid out in policies that are part of the REMIT information security framework are binding on all organisations providing, transmitting, storing or processing REMIT information without prejudice to relevant Union legislation and national legislation.

Any implementation guidance that is part of policies is binding only on the Agency and is not binding on other organisations.

A description of the structure of policy documents is presented in the chapter Structure of REMIT information security framework.

Structure of REMIT information security framework

The REMIT information security framework is defined with a set of policies represented in Figure 3 - Documentation of REMIT information security framework.

Each policy is structured as follows:

- Introduction
 - Scope
 - Applicability
 - Basic principles
 - Definition of terms and acronyms
 - References
- Responsibilities

- Requirements
- Implementation guidance

Basic principles and requirements laid down in each policy are applicable to collection, storing, processing and sharing of REMIT information and are binding on all organisations in scope.

Any implementation guidance is intended to assist in meeting the requirements and is binding on ACER and not binding on other organisations. Some requirements in the implementation guidance are presented in tables according to sensitivity marking level.

Note: Requirements listed under the implementation guidance for higher sensitivity marking levels are required in addition to all requirements listed for lower sensitivity marking levels. Empty requirement means no additional requirement to previous sensitivity marking level.

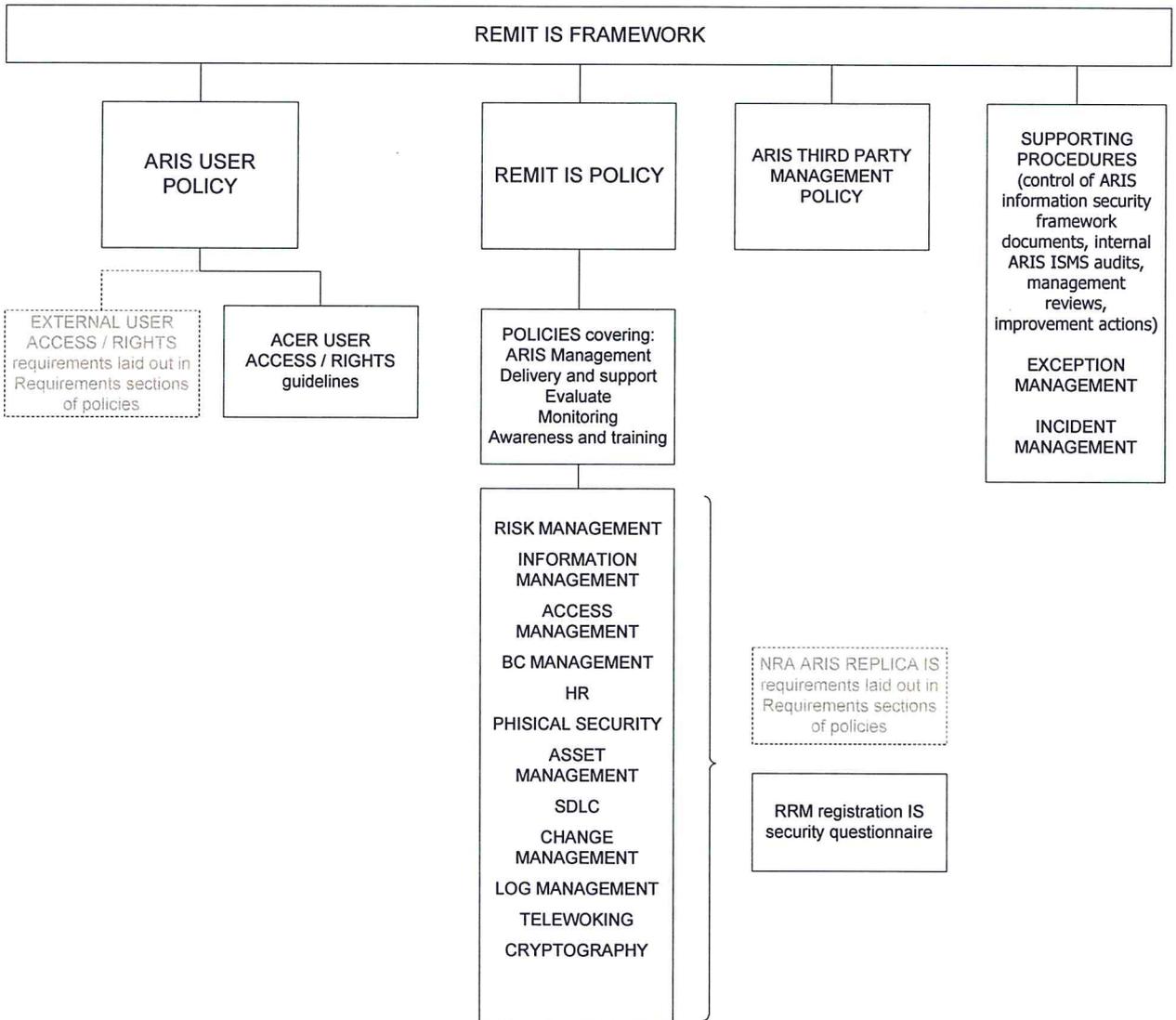


Figure 3 - Documentation of REMIT information security framework

Responsibilities

In each information security policy, responsibilities are described in a table defining requirements and responsible, accountable, consulted or informed (RACI) roles.

- R Refers to the person who must ensure that activities are completed successfully.
 In a RACI chart, answers the question: Who is getting the task done?
 Roles taking the main operational stake in fulfilling the activity listed and creating the intended outcome.
- A The individual, group or entity that is ultimately responsible for a subject matter, process or scope.
 In a RACI chart, answers the question: Who accounts for the success of the task?
- C Refers to those people whose opinions are sought on an activity (two-way communication)
 In a RACI chart, answers the question: Who is providing input?
 Key roles that provide input. Note that it is up to the accountable and responsible roles to obtain information from other units or external partners, too; however, inputs from the roles listed are to be considered and, if required, appropriate action has to be taken for escalation, including the information of the process owner and/or steering committee.
- I Refers to those people who are kept up to date on the progress of an activity (one-way-communication)
 In a RACI chart, answers the question: Who is receiving information?
 Roles who are informed of the achievements and/or deliverables of the task. The role in 'accountable', of course, should always receive appropriate information to oversee the task, as do the responsible roles for their area of interest.

Definition of terms

Term	Description
ACER Case management tool	ACER Information system for management and/or sharing of REMIT Case information.
ACER Case management tool data	REMIT case information stored, managed and/or shared in ACER Case management tool.
Additional national market monitoring data	Additional data (to REMIT information) collected, stored, managed on the basis of national law.
ARIS	Agency's REMIT Information System consisting of four tiers: Tier 1 – Data collection (including Centralised European Registry for Energy Market Participants and Notification Platform) Tier 2 – ARIS main database Tier 3 – Market monitoring system Tier 4 – The data sharing between the Agency and NRAs and other relevant authorities
ARIS data	REMIT information stored, managed and/or shared in ARIS (Data submitted by Registered Reporting Mechanisms from the external interface of ARIS, stops being ARIS data when leave outside interface of ARIS).
Information	Knowledge or data that has value to the organization or third party.
NRA market surveillance system	The market surveillance system operated by NRA to perform national market monitoring.

NRA market surveillance system data	Data collected, stored, managed within the NRA market surveillance system (REMIT information and Additional national market monitoring data).
REMIT Case information	Information related to the investigation of possible breaches of REMIT as compiled by the NRA or ACER within Article 16 of REMIT.
REMIT information	Any information collected, shared, managed for the purpose of REMIT including ARIS data and ACER case management tool data and REMIT case information.

Basic principles

1. The approach to REMIT information security is risk-oriented and conforms to international standards and/or established good practices.
2. The ARIS Information Security Management System follows ISO/IEC 27002 Code of practice for information security management, ISO/IEC 27010 Information security management for inter-sector and inter-organisational communications, and ISO 27005 Information security risk management and aims to satisfy ISO/IEC 27001 Information security management systems Requirements.
3. REMIT information in all forms shall be protected coherently and commensurately, from source through the Agency to recipients.
4. Security measures should be effective and consistent.
5. Information security awareness and education programme shall be established to provide stakeholders sufficient training to perform their responsibilities.
6. Deviations from this Information Security Policy and any security breaches shall be reported to the Agency⁴.
7. The Agency develops and manages the REMIT Information Security Management System (hereinafter REMIT ISMS). REMIT ISMS is a set of policies, procedures, guidelines and associated resources and activities, managed by the Agency with the purpose to protect information assets in scope of this policy.
8. The Agency establishes a group of representatives of national regulatory authorities and other competent authorities included in sharing of ARIS data. The Agency shall include this group in ARIS ISMS development.
9. The Board of Regulators is consulted on the REMIT Information Security Policy.
10. The Agency establishes a group of representatives of reporting parties. The Agency consults this group on ARIS ISMS requirements related to the submission of data to ARIS.
11. Managers at all levels are responsible for the implementation of the Information Security Policy and for ensuring staff adherence to the policy and guidelines.

⁴ See Information Security Exception Management and Security Incident Management policies for contact persons, responsibilities and means of communication.

12. All employees, temporary employees, third party employees and contractual workers are, according to their functions and authorities, responsible for observing the Information Security Policy.

ANNEX II: List of information security policies

- Information security
- Supporting procedures
- Exception management
- Incident management
- Risk management
- Information management
- Access management
- Business continuity management
- Human resources management
- Physical security
- Asset management
- System development life cycle
- Change management
- Service provider management
- Log management policy
- Teleworking
- Cryptography