Ref. Ares(2018)5584692 - 31/10/2018

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 787061

Advanced Tools for fighting Online illegal trafficking

D1.4 - Best practices and guidelines for handling ANITA resources

WP number and title	WP1 – Project Management
Lead Beneficiary	ENG
Contributor(s)	ALL
Deliverable type	Report
Planned delivery date	30/09/2018
Last Update	25/10/2018
Dissemination level	CO

Disclaimer

This document contains material, which is the copyright of certain ANITA contractors, and may not be reproduced or copied without permission. All ANITA consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

The ANITA Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Engineering Ingegneria Informatica	ENG	IND	IT
2	Centre for Research and Technology Hellas CERTH - ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	RTO	GR
3	Centro Ricerche e Studi su Sicurezza e Criminalità	RISSC	RTO	IT
4	Expert System S.p.A.	EXPSYS	SME	IT
5	AIT Austrian Institute of Technology GMBH	AIT	RTO	AT
6	Fundacio Institut de BioEnginyeria de Catalunya	IBEC	RTO	ES
7	Istituto Italiano per la Privacy	IIP	NPO	IT
8	SYSTRAN SA	SYSTRAN	SME	FR
9	Stichting Katholieke Universiteit Brabant	TIU-JADS	RTO	NL
10	Dutch Institute for Technology, Safety & Security	DITSS	NPO	NL
11	VIAS Institute	VIAS	RTO	BE
Law Enforcement Agencies (LEAs)				
12	Provincial Police Headquarters in Gdansk	KWPG	USER	PL
13	Academy of Criminalistic and Police Studies – Kriminalisticko-Policijska Akademija	AoC	USER	RS
14	Home Office CAST	CAST	USER	UK
15	National Police of the Netherlands	NPN	USER	NL
16	General Directorate Combating Organized Crime, Ministry of Interior	GDCOC	USER	BG
17	Local Police Voorkempen	LPV	USER	BE

To the knowledge of the authors, no classified information is included in this deliverable

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
V0.1	03/09/2018	Draft	[redacted]	First draft of table of content
V0.2	28/09/2018	Draft	[redacted]	Draft version for section 1 & 2
V0.3	22/10/2018	Draft	[redacted]	Contribution to Section 3. Protection Measures and Procedures for Accessing and Handling ANITA Resources
V0.4	25/10/2018	Peer Review	[redacted]	Deliverable passed internal peer review
V0.5	25/10/2018	Security Check	[redacted]	Deliverable passed security check
V1.0	25/10/2018	Final	[redacted]	Deliverable turned to final version
V1.1	31/10/2018	Final frozen	[redacted]	Some minor changes

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
CBRN	Chemical Biological Radiological Nuclear
DSA	Designated Security Authority
EUCI	European Union Classified Information
EURATOM	European Atomic Energy Community
FSC	Facility Security Clearance
NSA	National Security Authority
PSC	Personal Security Clearance
SAB	Security Advisory Board
SAL	Security Aspect Letter
SCG	Security Classification Guide

Table of Contents

List of Tables

Executive Summary

In ANITA, as well as in any research activities, information constitutes a material value for all types of projects and remains a crucial element for the ongoing of the activities and the achievement of the established objectives. Sensitive and classified information may be produced, accessed or exchanged during the project life and this is the reason why the very strict principles has been settled to this area. Loss or unauthorised access to this specific information (sensitive and classified information) may result in serious damage not only for specific organization or local society but, depend on classification level, but also to member states or to the European Union.

In fact, taking into consideration the sensitive nature of many security programs funded by the European Commission, and the involvement of many Law Enforcement Authorities, the ability and the reliability of individual participants to protect sensitive and classified information are indeed crucial for the **award** and **execution** of many security research programs. In particular, the multinational nature of large consortiums involving wide variety of partners from EU State Members, some specific rules can be hampered by the absence of unified wide regime for Security of Information.

The issue of security of information has been mentioned for the very first time in EEC Treaty signed in Rome in 1957 [1]. Initially, it gives to all State Members the right to secure specific information using individual methods. Over the years, this area has been not only organised but also, what is even more important, standardized for all EU State Members handling EUCI.

As a result of previous legislator steps in attempts of unification of sensitive and classified information area, the COUNCIL DECISION of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU) has been approved. On 15th October 2013 in the EU Official Gazette, L 274, the Council Decision dated 23rd of September 2013 on the Rules for protection of EU classified information (2013/488/EU) was published. The new rules revoked and replaced Decision 2011/292/EU dated 31st March 2011 on the Security Rules for protection of EU classified information. later on, new update by the COMMISSION DECISION (EU, EURATOM) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information in view of European Union has been approved. These are the very main act which provide guidelines for all European Union Classified Information (EUCI) and defining rules for areas such as: personal security, facility security, physical security of classified materials, etc.).

In the following section, a summary of security rules for protecting EU classified information will show the big picture of the measures that must be taken in order to handle EUCI, then specific focus will be highlighted in order to explain the security procedures and obligations under the Horizon 2020 research program, in particular with regards ANITA project.

Introduction

This deliverable focuses on defining the best practices in order to ensure the correct management of the project resources and results. It deals also with the establishment of the Security Advisory Board to assess the proper execution of security and protection measures and procedures for accessing and handling results of the ANITA project.

The deliverable is structured as reported below:

Chapter 1 – Security Framework and Provisions for Handling Security-Sensitive Information – provides a summary of security rules for protecting EU classified information showing the big panorama of the measures that must be taken in order to handle EUCI, then specific focus will be highlighted in order to explain the security procedures and obligations under the Horizon 2020 research program, in particular with regards ANITA project.

Chapter 2 – ANITA Security Advisory Board – describes the role of the Security Advisory Board, as well as the list of its composing members with respective curriculum.

Chapter 3 – Protection Measures and Procedures for Accessing and Handling ANITA Resources – the last chapter draws the conclusions and set up ANITA's measures and procedures that all involved members must comply with for accessing and handling ANITA resources.

1 Security Framework and Provisions for Handling Security-Sensitive Information

1.1 EU security rules for protecting EU classified information

In this section, we provide a general summary of the Commission Decision 2015/444/EC, EURATOM of 13 March 2015 on the security rules for protecting EU classified information [2].

1.1.1 Security classifications and marking

European Union classified information (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States. In other words, security measures applied for the protection of classified information are commensurate to the information's level classification. At the European level, there are four levels of classified information (European Union Classified Information – EUCI) depending on the degrees of prejudice their unauthorised disclosure may cause:

High	**TRES SECRET UE / EU TOP SECRET**	Information and material the unauthorised disclosure of which could cause **exceptionally grave prejudice** to the essential interests of the European Union or of one or more of the Member States.
Medium-High	**SECRET UE / EU SECRET**	Information and material the unauthorised disclosure of which could **seriously harm** the essential interests of the European Union or of one or more of the Member States.
Medium	**CONFIDENTIEL UE / EU CONFIDENTIAL**	Information and material the unauthorised disclosure of which could **harm** the essential interests of the European Union or of one or more of the Member States.
Low	**RESTREINT UE / EU RESTRICTED**	Information and material the unauthorised disclosure of which could **be disadvantageous** to the interests of the European Union or of one or more of the Member States

Table 1: Levels of European Union Classified Information – EUCI

All classified material must be affixed in a conspicuous manner by the originator of the material. The affixation informs recipients of the classification level and the degree of protection the material requires. Where documents are concerned, EUCI security classification stamps must always be affixed at the top and bottom of every page of the classified document.

1.1.2 Protecting classified information

Before access is granted, the service providing access has to verify whether the person in question is authorised, has the appropriate clearance level for access to classified information and is an addressee of such information.

1.1.2.1 *Personal Security Clearance*

Classified information is material that a body described as sensitive information that requires protection of confidentiality, integrity, or availability. Access is restricted by law or regulation to particular groups of people, and mishandling can incur criminal penalties and loss of respect.

According to EU rules for protecting EU classified information, Personal Security Clearance (PSC) can authorise an individual to access classified information starting from CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET up to TRÈS SECRET UE/EU TOP SECRET. However, for the RESTREINT UE/EU RESTRICTED classification level there is no need for PSC possession to be granted access to this kind of materials.

An individual shall only be authorised to access EUCI after:

a. His/her need-to-know has been determined;
b. He/she has been granted a PSC to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations;
c. He/she has been briefed on the security rules and procedures for protecting classified and sensitive information and has acknowledged his responsibilities with regard to protecting such information.

1.1.2.2 *Facility Security Clearance*

A facility security clearance (FSC) is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. The FSC may be granted at the Confidential, Secret, or Top-Secret level.

An FSC shall be granted by the National Security Authority (NSA) or Designated Security Authority (DSA) or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an industrial or other entity can protect classified information at the appropriate classification level within its facilities.

The following table summarises the EUCI access requirements for each classification level:

Classification level	Facility Security Clearance (FSC)	Personal Security Clearance (PSC)	Security briefing & acknowledgment	Need to know
EU RESTRICTED	No	No	Yes	Yes
EU CONFIDENTIAL	Yes	Yes	Yes	Yes
EU SECRET	Yes	Yes	Yes	Yes
EU TOP SECRET	Yes	Yes	Yes	Yes

Table 2: EUCI Access Requirements

1.1.3 Safeguarding Classified Information

It is essential that classified information be at all times properly safeguarded or stored in accordance with the minimum security requirements relevant to the level of classification. For this reason, all information

classified at EU CONFIDENTIAL and above **MUST** be stored only in secure facilities that have obtained a facility security clearance.

1.1.4 Consulting Classified Information

It is the responsibility of cleared individuals to safeguard classified material at all times. While in use, classified information should be given sufficient protection to reasonably prevent against loss or compromise. As a starting point, all cleared or authorised individuals must be aware that classified information cannot be discussed over unsecured telephones, in public places, or in any manner that might allow transmittal or interception by unauthorised persons. This includes not working on classified material on unapproved computers. Classified information should never be left unsecured or unattended. Constant surveillance by an authorised individual who is able to exercise direct control over the classified material provides additional security. The authorised individual must, however, have the appropriate clearance and need-to-know, and must take action to prevent access to the material when others who do not have the appropriate clearance and need-to-know are present.

Working with classified information at the level of EU CONFIDENTIAL outside the secure facilities is **PROHIBITED**. When working with classified information at the level of EU-RESTRICTED on an approved computer but in an unsecured area, any open curtains or doors should be closed. It is prudent to also post a "DO NOT DISTURB" sign. If a visitor or unauthorised individual is present, a classified document must be protected by either covering it, turning it face down, or placing it in an approved storage container.

Classified material should never be taken home. In general, classified information should be stored after it has been used.

When not in use, classified information is to be properly secured in an approved container, unless it is being guarded by another properly cleared person with a need-to-know. The storage of classified material in anything other than an approved container is strictly prohibited. Approved storage containers should remain locked.

EU-RESTRICTED material **may** be stored in normal steel cupboards by the holders of such information. EU-CONFIDENTIAL and above materials may not be stored outside the cleared secure facilities.

1.1.5 Reproduction of Classified Material

Copies of classified information are subject to the same security controls as original classified material. Copies of classified information may only be reproduced by an authorised service for the purposes of consultation in a meeting in camera and is limited to EU-CONFIDENTIAL information and below.

For a meeting in camera with EU-RESTRICTED classified information, the secretariat responsible for the meeting is responsible for strictly applying the rules to:

- produce and register the necessary numbered copies;
- distribute only the necessary number of copies, which meet the number of authorised individuals; and
- recover the copies at the end of the meeting to ensure proper storage or destruction.

For a meeting in camera with EU CONFIDENTIAL information, the Classified Information Unit will hand over to the responsible secretariat the registered and exact number of copies needed together with an handling

and receipt list of these copies. The secretariat responsible for the meeting has to ensure all copies are complete and returned to the Classified Information Unit at the end of the meeting.

Copying classified documents on office photocopiers is **PROHIBITED** unless, in the case of EU-RESTRICTED documents, allowed by the originator, the machines are certified, disconnected from the network, have no hard disk and, proper controls are in place.

1.2 Horizon 2020 security-related obligations

Horizon 2020 [3][4] security-related obligations concern:

- Security recommendations;
- Data or information used or produced by a research project which requires protection against unauthorised disclosure (classified information);
- Dual-use goods or dangerous materials and substances (subject to export- or transfer control);
- Information or materials subject to national security restrictions.

1.2.1 Security scrutiny

Proposals dealing with information that is EU-classified under the Commission's internal Rules of Procedure are subject to security scrutiny.

a. When are proposals subjected to security scrutiny?

As stated in the H2020 Grants Manual [5], the following proposals are subject to security scrutiny:

- All proposals belonging to topics in the Secure Societies WP;
- All proposals belonging to calls or topics marked potentially security sensitive;
- Proposals of any other WP, call and topic marked as raising (potential) security issues by the applicant;
- Proposals identified as raising (potential) security issues by the responsible Project Officer or Call Coordinator;

b. How are proposals scrutinised for security?

The scrutiny check is not a full security check on all the aspects of a project which might have a bearing on security. It simply identifies projects involving information that is sensitive from the security point of view and, where appropriate, classes their deliverables as classified deliverables.

Security scrutiny may lead to **Security Requirements**. If applicable, these are included in the grant agreement as a Security Aspect Letter (SAL) and the annexed Security Classification Guide (SCG).

Security scrutiny does not relate to activities involving dual-use goods or dangerous materials and substances. Security scrutiny applies to most parts of Societal Challenge (Secure Societies), but it may also apply to other proposals, e.g. if:

- the applicants state in the submission forms that the proposal is security-sensitive (i.e. that it involves EU-classified information);
- the work programme flags up the topic as one that could result in security sensitive projects;
- the Commission detects or suspects that: classified information is being used as background or the project will generate classified information.

c. How is the security scrutiny process organised?

Scrutiny is the responsibility of the Security Scrutiny Working Group, comprising experts appointed in close cooperation with the relevant Programme Committee and the competent national security authorities. It is chaired by a Commission representative (DG Home). Classification of information used in and/or produced by research projects will normally depend on two parameters:

a. the **subject** of the research results (i.e. explosives, CBRN, infrastructure and utilities, border security, intelligent surveillance, terrorism, organised crime, digital security and space).
b. the **type** of the research results (i.e. threat assessments, vulnerability assessments, specifications, capability assessments, incidents/scenarios).

1.2.2 Results and implications of security scrutiny

As specified before, if necessary, a Horizon 2020 proposal undergoes the security scrutiny during the evaluation phase. In this case the Security Scrutiny Working Group will determine the level of sensitivity of the proposal and check whether all security aspects are being handled appropriately.

According to H2020 Security Related Obligations [6], the EC informs the consortium of the outcome of the security scrutiny at the beginning of the grant preparation phase or as soon as possible afterwards. The possible outcomes are:

- Classification is not necessary;
- Classification is not necessary, but recommendations for the grant agreement preparation;
- Classification is necessary;
- The proposal is too sensitive to be funded.

a. Classification not necessary:
The project will be handled in the same way as all the others under the same call for proposals. No further action is needed.

b. Classification is not necessary, but recommendations for the grant agreement preparation:
The project will be handled in the same way as all the others under the same call for proposals. However, specific security recommendations are issued and inserted under Article 37.1 in the Grant Agreement.

c. Classification necessary
In such cases, security requirements are incorporated in Annex 1 to the grant agreement. These requirements and the project's level of security classification are set out in the Security Aspect Letter (SAL) and the Security Classification Guide (SCG) annexed to it.

d. Proposal too sensitive to be funded
Security scrutiny may reveal that the information to be used or generated by the project is too sensitive, or that the applicants lack the right experience, skills or authorisations to handle classified information at the appropriate level. In such cases, funding is refused and the proposal rejected.

1.2.3 Classification parameters under research programmes

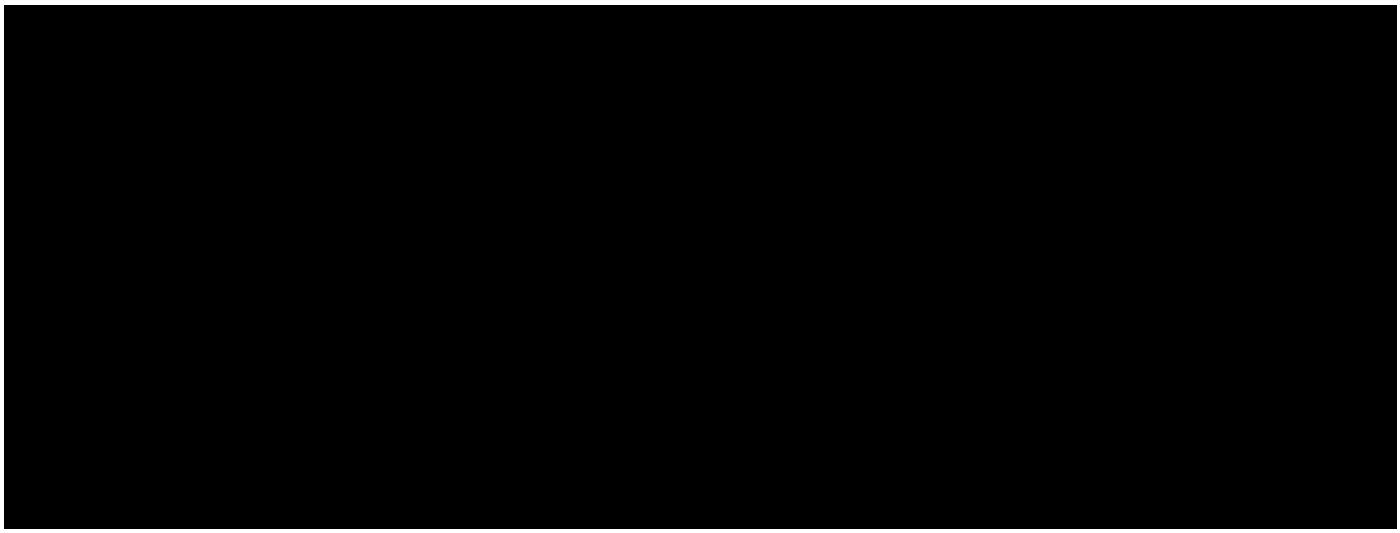
The classification of information produced by the originator of the material will normally depend on two parameters:

i. the **subject-matter**:

- explosives
- CBRN
- critical infrastructure and utilities
- border security
- intelligent surveillance
- terrorism
- organised crime
- digital security
- space

ii. the **type** of the research/results and whether it is being done in simulated environments or in real world experimentation:
   - **threat assessments** (i.e. estimation of the likelihood of a malicious act against an asset, with particular reference to factors such as intention, capacity and potential impact);
   - **vulnerability assessments** (i.e. description of gaps or weaknesses in networks, services, systems, assets, operations or processes which can be exploited during malicious acts, and often contain suggestions to eliminate or diminish these weaknesses);
   - **specifications** (i.e. exact guidelines on the design, composition, manufacture, maintenance or operation of threat substances or countermeasure substances, technologies and procedures);
   - **capability assessments** (i.e. description of the ability of an asset, system, network, service or authority to fulfil its intended role — and in particular the capacity of units, installations, systems, technologies, substances and personnel that have security-related functions to carry these out successfully);
   - **incidents/scenarios** (i.e. detailed information on real-life security incidents and potential threat scenarios:
     - on past incidents (often including details not otherwise publicly available, demonstrating the real-life effects of particular attack methods or security gaps which have since been addressed);
     - on devised scenarios (commonly derived directly from existing vulnerabilities, but normally with a lower level of detail, particularly of the attack preparation phase).

These categories are not exhaustive, and may overlap.



[redacted]

1.3.2 ANITA security obligations setup in the grant agreement

1.3.3 Security staff

In ANITA, a Project Security Officer has been designated and a Security Advisory Board will be constituted in order to ensure the correct management of the project resources and results in terms of information sensitivity and security measures.

1.3.4 Security Advisory Board

In ANITA, a Security Advisory Board (SAB) has been established and is chaired by the Project Security Officer and includes 3 additional members with sufficient knowledge and experience in security issues.

1.3.5 Limited dissemination

In ANITA, for security and sensitive data reasons, a predefined list of deliverables with confidential dissemination level has been established. This list has been updated to include the 3 deliverables recommended after the security scrutiny (1.3.1). It is important to note that confidential dissemination means limited dissemination to only EC and Members of the ANITA consortium, and does not mean EU CONFIDENTIAL Classification.

2 ANITA Security Advisory Board

2.1 Role of the Security Advisory Board

The Security Advisory Board (SAB) will assess the proper execution of security and protection measures and procedures for accessing and handling, results of the ANITA project. SAB will monitor regularly the project activities and assess the sensitivity of information handled by participants providing continuously support to the consortium.

The process for reviewing all ANITA deliverables will be integrated with the quality review process put in place and described in the internal report Project Quality Plan.

Specifically:

a. any deliverable will be reviewed by the SAB in order to assess the lack of sensitive information;
b. any deliverable will be reviewed in order to assess the correct level of classification and in case to accordingly propose the upgrade/downgrade;
c. when applicable, the table of contents of the deliverables will be also reviewed by the SAB;
d. the review by the SAB will be included in the history of all deliverables.

[redacted]

[redacted]

4 Conclusions

The flow and handling of information during the research process is crucial not only for the effectiveness of the project management, but also for final results of the research activities and objectives. All contributors of the ANITA project have been informed and briefed about the procedures and legal obligations with regards ANITA security measures as well as EUCI handling measures in general. ANITA management structure is perfectly organized and all participating partners have committed to comply with ANITA security measures under the control and monitoring of the Security Advisory Board (SAB).

The process of generating, exchanging and handling of information have been deployed, and will be realised under the monitoring of the SAB. In addition, the SAB will monitor regularly the project activities and assess the sensitivity of information handled by participants providing continuously support to the consortium. The process for reviewing all ANITA deliverables has been integrated with the quality review process put in place and described in the internal report Project Quality Plan.

5 References

[1] The Treaty of Rome, 25 March 1957

[2] COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information

[3] Security Notice 02 - The creation, handling, distribution, storage and destruction of RESTREINT UE/EU RESTRICTED information, 16/03/2015

[4] H2020 Programme - Guidelines for the classification of information in research projects

[5] Horizon 2020 H2020 Grants Manual - http://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/from-evaluation-to-grant-signature/grant-preparation_en.htm

[6] Security-Related Obligations – Infoday 6 March 2017 - [redacted]

[7] ANITA Security Evaluation Summary Report