

# **POLICY FOR INFORMATION AND DATA** **SECURITY AND CONFIDENTIALITY**

## **DISTRIBUTION**

<b>Copy No.</b> <b>1</b>	<input checked="" type="checkbox"/> <b>Controlled for internal use</b>	<input type="checkbox"/> <b>Controlled for external use</b>	<input type="checkbox"/> <b>Uncontrolled</b>
-----------------------------	--	---	--

### **Table of contents**

1. INTRODUCTION .....	2
2. GENERAL RULES AND INSTRUMENTS FOR DATA AND INFORMATION SECURITY AND CONFIDENTIALITY .....	2
Employees, contractors and collaborators duties .....	2
Information Technology Infrastructure .....	2
EuCI Web Site .....	2
Physical Security Measures .....	2

### **Revision History**

<b>N.</b>	<b>Date</b>	<b>Reason</b>	<b>Author</b>	<b>Verified and Approved</b>
00	2011-03-21	First issue	QD	DIR
01	2014-03-28	Three years revalidation cycle, no changes in the document	QD	DIR
02	2021-02-04	Revalidation cycle, no changes in the document	QD	DIR

## 1. INTRODUCTION

EuCI regards at all the information obtained from any source, or created during the performance of its activity, as one of its most important assets. All the information related to customers, personnel, suppliers and any other entity, excluding that of public domain and explicitly defined as non-confidential in EuCI procedures and contractual documents, is considered confidential.

With this policy EuCI states general rules and instruments to preserve security and confidentiality of information. This policy should be integrated, if necessary, by any other document requested by local regulations about information security and confidentiality in each state where EuCI operates.

## 2. GENERAL RULES AND INSTRUMENTS FOR DATA AND INFORMATION SECURITY AND CONFIDENTIALITY

### Employees, contractors and collaborators duties

- All EuCI employees shall sign a non-disclosure agreement about any information they deal with
- All EuCI Impartiality Committee members shall sign a non-disclosure agreement about any information they deal with during the Committee activity
- All EuCI suppliers, contractors and any entity acting on EuCI's behalf, shall sign a non-disclosure agreement about any information (about EuCI, EuCI clients, etc.) they deal with
- All EuCI personnel shall be trained about Information security and confidentiality procedures
- Auditors shall send to EuCI headquarter all the information about audit or preliminary visit as soon as possible after the event, following EuCI instructions.

### Information Technology Infrastructure

- EuCI Information Technology services and hardware suppliers shall certify compliance of EuCI IT infrastructure to local regulations and laws about data security and confidentiality and to this policy document.
- EuCI IT Infrastructure shall be protected by automatically updated anti-malware hardware and software.
- EuCI IT infrastructure shall have controlled and restricted access.
- EuCI Employees and External collaborators, e.g. Auditors, shall have access only to information related to their activity.
- All digital information is protected from accidental loss by automatic back up, executed at least once a day.

### EuCI Web Site

- EuCI Web site information shall be adequately protected against hackers attack.
- Client and procedural information published on EuCI web site shall be updated within one day.

### Physical Security Measures

- All paper documents shall be securely archived.
- All EuCI sites shall be protected with anti-theft and fire protection systems.