

MEMORANDUM OF UNDERSTANDING

on the establishment of a secure communication line

between

the European Police Office



and

the International Criminal Police Organisation - INTERPOL



The European Police Office

Represented for the purposes of this Memorandum of Understanding by Mr Rob Wainwright, Director, and hereafter referred to as 'Europol',

and

The International Criminal Police Organisation – INTERPOL

Represented for the purposes of this Memorandum of Understanding by Mr Ronald K Noble, Secretary General, and hereafter referred to as 'INTERPOL',

Hereinafter collectively referred to as the 'Parties' or individually as the 'Party',

Having regard to the Agreement between Europol and INTERPOL signed on 5 November 2001 (hereinafter referred to as "the Agreement"),

Whereas transmission of information between the Parties on the basis of the Agreement requires the establishment of a secure communication line between them.

Whereas the establishment of an interconnection between the Europol Secure Network and the INTERPOL Secure Network (I-24/7) has been put forward as a means to developing a secure communication line,

Have agreed as follows:

Article 1
Purpose and Scope

The purpose of this Memorandum of Understanding is to regulate the establishment, implementation and operation of a secure communication line for the transmission and exchange of information between Europol and INTERPOL within their respective mandates and legal frameworks and in accordance with the Agreement.

The establishment of the said secure communication line shall be done via interconnection of both Parties' secure networks.

This Memorandum of Understanding does not confer direct access rights to Europol or INTERPOL databases, applications or services. Subsequent Bilateral Agreements shall define which applications and services can be used via the secure communication line.

Via the exchange of letters, written arrangements shall be made relating to the access of categories of users to specific applications and services available via the secure communication line, in accordance with the legal framework concluded between the Parties.

RW

This Memorandum of Understanding does not restrict the possibilities of the Parties to implement measures in their own network to further enforce access restrictions to applications and services.

The establishment of the secure link does not affect in any way the tasks and working methods of the Liaison Officers as described in the Memorandum of Understanding as mentioned in Article 4(1) of the Agreement between Europol and INTERPOL.

Article 2 **Transmission of information**

1. Transmission of information between the Parties shall only take place in accordance with the Parties' respective legal frameworks and the relevant provisions of the Agreement.
2. The transmission of classified Europol information using the secure communication line is limited to the level of RESTREINT UE – EU RESTRICTED - and its equivalent at INTERPOL.
3. The transmission of classified INTERPOL information using the secure communication line is limited to the level of INTERPOL restricted and its equivalent at Europol.

Article 3 **Code of Connection**

1. Both Parties undertake to implement minimum standards for security established in Annex 1: Code of Connection. Both Parties confirm that they have protected the connecting systems to the baseline standard with policies and technologies configured appropriately and have considered the controls established in this Annex.
2. By signing this Memorandum of Understanding, both Parties confirm their compliance with the code of connection provided in Annex 1.
3. In the event that one Party substantially deviates from the principles and concepts defined in this Article or Annex 1, then services between the two networks may be terminated until the issues have been resolved.
4. Both Parties agree that, if they make an onward interconnection to any other network, then such a connection must be subject to a similar agreement (code of connection) that will ensure the security baseline.
5. Both Parties agree not to interfere with the ICT equipment of each Party, including (dis)connecting cables or equipment unless specifically instructed or in the case of an emergency.

RN
[Signature]

6. Should a serious security incident occur, e.g. a virus infection, it is expected that the Party must consider disconnecting from the other Party's system to protect the further spread of any infection.
7. Before any modifications to networked systems impacting on the other Party's network, or the interconnections, are implemented, information and sufficient advance notice must be provided in writing to the Head of the Capabilities Department when the modification impacts Europol, and to the Head of the Network Branch of the Infrastructure sub-directorate of the Information System Directorate when the modification impacts INTERPOL. Should a meeting be required to discuss the modifications this should take place prior to any implementation.
8. Each Party is responsible for the security of its own systems from the demarcation point onwards.
9. Both Parties agree not to perform any type of tests, vulnerability scans or intrusions into the others' systems without prior authorisation in writing.
10. Both Parties agree to share information pertaining to threats and vulnerabilities that may interfere with each other's systems.
11. Europol equipment installed on the premises of INTERPOL remains the property of Europol. INTERPOL's equipment installed on the premises of Europol remains the property of INTERPOL. The equipment owner is responsible for its security; however bilateral arrangements which deviate from this principle may be made depending on circumstances.
12. Each Party is responsible for the maintenance of its own equipment. Support requests may be made to system administrators of each Party's respective network in order to facilitate support and maintenance issues. A procedure to handle such requests will be developed on a bilateral basis between Europol and INTERPOL.

Article 4

Purchase, maintenance and distribution of costs

1. In accordance with its procurement rules, Europol shall purchase all goods and services necessary for the establishment, implementation and operation of the secure communication line.
2. The costs of the establishment of the secure communication line shall also be paid by Europol. The secure communication line and all equipment connected to it are supplied by, and remain the property of, Europol.

RN
Ren

3. Europol shall be responsible for maintenance of the secure communication line and, if necessary, for replacement of defective equipment. In accordance with the applicable procedures, INTERPOL shall not unreasonably deny access to the relevant areas of its premises to any personnel designated by Europol for such maintenance and replacement of defective equipment. In case physical entry into INTERPOL premises is required, EUROPOL shall provide INTERPOL with the names and other information that INTERPOL routinely requires of visitors in order that the necessary security checks can be carried out in a timely manner. In case a malfunction is detected by INTERPOL, Europol User Support personnel shall be the first line of technical assistance.
4. The monthly running costs for the secure communication line shall be paid by Europol.
5. Should the secure communication line be dismantled, INTERPOL shall transfer to Europol the items registered as Europol's assets.

Article 5 **Liability and settlement of disputes**

1. Without prejudice to Article 12 of the Agreement, a Party shall be liable for damage caused to the other Party as a result of the establishment, implementation or operation of the secure communication line. In such cases, the Parties shall endeavour to find an equitable solution for the compensation of damages suffered.
2. Any dispute between the Parties concerning the interpretation or application of this Memorandum of Understanding shall be settled in accordance with Article 13 of the Agreement.

Article 6 **Amendments**

Amendments to the Memorandum of Understanding shall be mutually agreed upon by exchange of letters between the Parties.

Any changes relating to job titles and contact details stated in this Memorandum of Understanding and Annex 1 shall be notified to the other Party without delay.

Article 7 **Termination**

The Memorandum of Understanding may be terminated, upon three months' written notification, by either of the Parties.

RW
RW

Article 8
Entry into force and signatures

The Memorandum of Understanding shall enter into force on the first day of the month following signature by the last Party.

Signed in duplicate

For Europol

**For the International Criminal Police
Organisation - INTERPOL**



Mr Rob Wainwright
Director



Mr Ronald K Noble
Secretary General

on 11/10/11 (date)
in Lyon (place)

on 11/10/2011 (date)
in Lyon (place)

Annex 1: Code of Connection

1.1. Introduction

This code of connection applies to the interconnection of the Europol Secure Network and INTERPOL Secure Network. "Europol" and "INTERPOL" are hereafter referred to as "the Parties".

The primary purpose of this Code of Connection (CoCo) is to provide assurance that the two interconnected networks are adequately protected against threats to confidentiality, integrity and availability and to minimize the risk that a security incident in the network of one Party could potentially affect the network of the other Party. It is therefore important that a baseline set of security measures are agreed between the Parties.

The key principle of this Code of Connection is that both Parties shall take steps to actively manage the security of their networks and to implement a minimum set of security controls. The aim of such a security baseline is to reduce security risks and prevent security incidents in one of the Party's network from impacting the other's network. Each Party is responsible for the security of its own systems.

This Code of Connection is binding upon both Parties.

1.2. Minimum Security Controls

1.2.1. Europol and INTERPOL Secure Network System Specific Security Requirements

Europol maintains a list of network infrastructure security requirements in a document entitled "Europol Secure Network System Specific Security Requirements (SSSR), File No. 2750-152" whereas INTERPOL maintains its Information Security Policy.

The Europol SSSR is a complete and explicit statement of the security principles and detailed security requirements to be met by a system. It is based on the key security principles established by the Europol Security Manual and the result of the risk assessment of the Europol Secure Network.

The INTERPOL Information Security Policy framework defines INTERPOL's Information Security Management System (ISMS) that ultimately leads to the implementation and operation of security controls based upon an assessment of risks that could impact INTERPOL.

The INTERPOL Information Security Policy defines the network security objectives that must be achieved, and individual INTERPOL Information Security Standards define more technical characteristics and requirements of security measures used to achieve these objectives.

Both documents are subject to regular review and in general aim to achieve similar security objectives. In the case that future revisions of either document are likely to cause conflict with the other, then an amicable agreement shall be found and a common security measure proposed.

A mandatory requirement for interconnection of the Europol network to another network is that those responsible for managing the other network and Europol must implement policies, procedures and technical measures that are comparable to those mentioned in the SSSR document. This is the same principle as the INTERPOL Information Security Policy that defines the management system for information security within INTERPOL.

The actual procedures or technologies defined in these documents do not have to be the exactly the same as used by one or the other organisation, however the concepts mentioned within both documents must be addressed according to each organisation's rules, regulations and constraints.

This approach is in line with article 2 of Europol's Rules on the Confidentiality of Europol information, in which the principle is established that Partner Agencies undertake to ensure that all information which is processed by or through Europol shall receive a level of protection which is equivalent to the protection afforded by Europol to such information. It is also compliant with INTERPOL's "Implementing Rules on the Processing of information for the purposes of International Police Cooperation" that state "National Central Bureaus and international authorized entities shall be responsible for adopting an appropriate level of security at least equivalent to the minimum level of security laid down in the security policies established by the General Secretariat".

1.2.2. Baseline Measures

The Europol Secure Network SSSR and the INTERPOL Information Security Policy should be used as a guide to define control measures for the respective networks. In principle, both Parties may choose to implement the measures which are appropriate in accordance with local security policies and regulations to address the threats and concepts mentioned in these documents. However, in order to ensure a minimum level of security assurance, the control measures listed below are a baseline for network interconnection. The acceptance of this code of connection implies the acceptance of the baseline physical, technical and procedural security measures mentioned below.

RN
RV

1.2.2.1.Procedural Controls

Both Parties agree to employ the following minimum procedural controls:

- Users of the system must be security cleared to the appropriate level.
- An authentication policy, i.e. baseline guidelines for password construction and management, must be in place.
- A policy for any remote access and appropriate authentication measures should be in place.
- Accounting and audit measures must be in place.
- Information relating to security incidents that have the potential to interfere with the security of the other Party's network should be reported to either Party as soon as possible. An example of such security incidents is included in section 1.3 below. Security incidents should be reported to:

INTERPOL: INTERPOL Information Security Incident Response Team
isirt@interpol.int or telephone +33 4 72 44 73 54 or +33 4 72 44 73 71

Europol: C12 Network & Operations Centre (ITOC), c12@europol.europa.eu

1.2.2.2.Technical Controls

Both Parties agree to employ the following appropriately configured technical controls:

- Boundary (perimeter) security devices such as firewalls or screening routers.
- Anti-virus technologies supported by an anti-virus policy and strategy.
- No workstation directly connected to a public computer network such as the Internet may be connected to the Europol Secure Network or used to access the Europol Secure Network.
- Systems that are indirectly connected to a public network such as the Internet must be appropriately protected in order to protect both networks from such a public network.
- Encryption of traffic when public communication lines are used between the networks, such an encryption technology, must be of an appropriate strength for the classification of data that it is intended to protect.
- Information security assessments and tests are carried out to ensure that vulnerabilities are identified and remedied.
- Networks are checked for compliance with the respective organisation's appropriate security rules or policies on a regular basis.



1.2.2.3. Physical Controls

Both Parties agree to the following physical controls:

- Network equipment and components that are not otherwise protected must be located in an appropriately physically-secure location.
- Sensitive equipment such as consoles, server equipment, firewalls, network switches and encryption devices must employ physical access control (e.g. be located in a locked room).
- Access to workstations, terminals, etc, where the potential to access the others' network exists, must be physically restricted. Where workstations need to be located in a publicly accessible area for organisational or operational reasons, such equipment must be physically protected at all times from unauthorised access, theft or loss. For example, such equipment must not be left unattended in public places.

1.3. Examples of Security Incidents

The following is a list of examples that may generate a security alert and potentially lead to a security incident. As a minimum, such events should be investigated and, where appropriate, notified to the other Party so that they can check that no compromise of confidentiality, integrity or availability of their information has occurred or will potentially occur.

- The power goes down. For some reason the UPS does not respond. Critical systems are down.
- A serious virus or other malware incident.
- Loss or theft of equipment that contains information belonging to the other Party or may contain information that could lead to unauthorised access to the other Party's network.
- A log-check or intrusion detection system reveals suspicious patterns of activity.
- The log of the physical access control system shows unusual activity, e.g. a staff member's coded badge is used frequently for entering the building at night when the holder should only be working nine-to-five, and this activity had not been authorised.
- There have been several sustained attacks on key network components or hosts.
- At a routine check, it appears that a normal user has been granted administrator privileges.
- A system is not responding during normal working hours and there is no authorised reason for the system to be unavailable
- Key security rules, such as a firewall configuration, are found to be not compliant with the relevant security policy.
- Any other incident whereby there is a potential or actual threat to the other Party's network or information.

12
22