

2016/14/2017
TBS



CEDEFOP

European Centre for the Development
of Vocational Training

RES/CFL/TBG/ASAIN/2012/005

CEDEFOP SECURITY POLICY

[Handwritten signature]

1. Introduction

This Cedefop Security policy sets out the security principles and implementing measures to safeguard security at Cedefop (e.g. security of persons and infrastructure, document and information security etc). The principles and standards laid down in this security policy build on the corresponding systems set up by the European Commission. At the same time, mindful of the need to strike a balance between adequate security and operational flexibility, we have adapted these principles and measures to the mission and scale of Cedefop.

The policy is divided into five parts:

- Part I sets out the principles and organisation of security within Cedefop.
- Part II describes the security measures which deliver a level of basic protection.
- Part III lists the additional measures required for the protection of more sensitive information.
- Part IV contains provisions on the security of information handled in information technology and communication systems.
- Part V: procedures for dealing with breaches of security.

The policy covers all practical aspects of our work, including, for example, information exchange, staff, organisation and planning, administration and technical activities and infrastructure. It aims to create a working environment within Cedefop where we are all security conscious. The introduction of the policy is, therefore, accompanied by training and instructions on security issues for all Cedefop staff.

The creation and maintenance of a secure working environment is the individual and shared responsibility of all staff members. Integrating these principles into our work habits will be key to the success of this policy and we count on each one of you in its implementation.

PART I: PRINCIPLES AND ORGANISATION OF SECURITY

CHAPTER I.1. — Definitions and objectives of security

I.1.1. Definitions

For the purposes of the Cedefop security policy:

- (a) 'Third party' means a body, which is not part of Cedefop;
- (b) 'Cedefop Security Committee' or 'Security Committee' means Committee consisting of representatives of Cedefop appointed by the Director of Cedefop, with the task to decide and approve the security policies of Cedefop;
- (c) 'Cedefop Security Coordinator' or 'Security Coordinator' means the Head of Resources who coordinates and controls matters of security;
- (d) 'Cedefop Security Officer' or 'Security Officer' means Cedefop officer appointed by the Director as the official responsible for security issues. He or she designs and implements policies to be adopted/approved by the Head of Resources;
- (e) 'Cedefop classified information' and 'Cedefop classified documents' means information or documents subject to additional security measures as outlined in Part III of this policy, and marked with the classification level 'Cedefop Confidential'
- (f) 'Governing Board' means the Governing Board of Cedefop;
- (g) 'Processing of information' ('processing') means any operation or set of operations which are performed on personal or non-personal data, whether by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- (h) 'Breach of security' means any act or omission contrary to a provision of the security policy which might endanger or compromise Cedefop security. Compromise of information occurs when it has wholly or in part fallen into the hands of unauthorized persons.
- (i) 'Host State' is the Member State which hosts Cedefop: Greece;
- (j) 'Cedefop staff' means officials, temporary agents, contract agents, and national experts on secondment, employed and working at Cedefop;
- (k) 'Cedefop external contractors' means staff provided by external contractors working at Cedefop.

I.1.2. Objectives of security

The Cedefop security policy aims:

- to protect all persons working at Cedefop premises.
- to safeguard all Cedefop premises from damage, unauthorized access or other threats;
- to safeguard installations housing Cedefop information from sabotage and malicious willful damage;
- to safeguard Cedefop information handled in communications and information systems and networks against threats to its integrity and availability;
- to safeguard Cedefop information from unauthorized disclosure;

I.1.3. Threats and risk assessment

The security of Cedefop depends on the continuous monitoring of the perceived threats to the organization, its staff and its information systems. The Security Officer keeps an incidents log

4

for this purpose¹. The results of this monitoring support the potential threat and risk assessment and the necessary adjustments to policy and practice. The Security Officer is responsible for the monitoring and assessment and may consult the national Security Services of the host country and other sources as necessary.

The Security Officer works under the supervision of the Security Coordinator. The Security Officer regularly reports to the Security Coordinator on evolving threats and proposes remedial actions. The Security Coordinator makes these reports available to the Security Committee, and report to that Committee on follow up actions by Cedefop.

CHAPTER I.2. — Organization of security in Cedefop

I.2.1. The Security Coordinator

The Security Coordinator has the general responsibility, coordination and control for all issues relating to security. He or she approves security policies, upon proposal of the Security Officer and after consultation with the Security Committee.

I.2.2. The Security Committee

The Security Committee is consulted for the adoption of the security policies. The Security Committee includes a staff appointed by the Director, a staff appointed by the Staff Committee and is chaired by the Security Coordinator (Head of Resources). The Security Officer attends the meeting as an observer. A simple majority of persons present is sufficient for the deliberation.

I.2.3 The Security Officer

The Security Officer ensures the monitoring and the practical implementation of all the security measures laid down in this Cedefop Security policy. He or she informs and advises the Security Coordinator on any related issues, both at his/her own initiative and on request.

The Security Officer is responsible for the day-to-day activities of Cedefop staff assisting with security and external guards.

The Security Officer cooperates, when appropriate, with the competent authorities of the Host State of Cedefop. Except in emergencies, such cooperation requires prior authorization from the Security Coordinator.

I.2.6 The Data Protection Officer

The Data Protection Officer advises the Security Officer on data protection requirements with a view to ensuring compliance with all policies and regulations required in this area.

¹ The incident log contains date, name and description of the incident

PART II: BASIC SECURITY MEASURES

CHAPTER II.1. — PHYSICAL SECURITY

II.1.1. CEDEFOP premises

Cedefop is under constant electronic and human surveillance. A sufficient number of security guards² must be present on the premises at all times.

Entrance to and exit from Cedefop premises is only granted through monitored entrances/exits and is subject to authorisation. The Security Officer, under the supervision of the Security Coordinator, is responsible for ensuring that all necessary physical protection measures are taken to prevent unauthorized access to Cedefop premises. These measures aim to limit opportunities for attacks on the premises or to minimize the effect of such attacks.

II.1.2 Access

All persons accessing Cedefop premises may be asked to undergo a security check, by the Security guard at the entrance Security booth..

Access for Cedefop staff members is regulated in administrative circular No. 2008/1.

On decision by the Directorate, persons may be denied access to Cedefop in general. In cases of emergency such a decision may be taken preliminary by the Head of Resources. It should be later on confirmed by the Directorate. A list of such persons should be communicated to the Security Coordinator, the Security Officer and the Security guards. These persons are denied access even if invited staff members or if in possession of an access card.

1.2.1 Service Card Holders

All Cedefop staff, external contractors and trainees are issued an access card by the Security Officer, enabling them to have automatic access to and exit from Cedefop buildings.

The loss of an access card must be reported immediately to the Security Officer. The access card remains the property of Cedefop at all times. It is forbidden to copy access cards. Replacement of lost access cards will be provided by the Security Officer or – in his/her absence – by his or her substitute.

All accesses to and exits from Cedefop buildings by way of access cards are logged in a separate data file, managed under the responsibility of the Security Officer, in accordance with the applicable data protection rules.

1.2.2 External Visitors

The names (and functions where appropriate) of all external visitors must be provided to the Security Guards beforehand. In case of official visits by high ranking Officials, the Security Officer must be informed beforehand. The Security Officer will inform the Security Guards about the visit and of any additional security measures that are considered necessary.

All external visitors should:

- a) Present themselves with proof of identity at the Security booth;
- b) Obtain, a temporary VISITOR card;
- c) The Security guards should contact the inviter and arrange for the visitor to be met at the reception.

² This is normally a service provided by an (external) contractor.

- d) The organiser must provide staff to greet the external visitors and accompany them to the meeting room;
- e) External visitors are not allowed unaccompanied access to the Cedefop building.
- f) Visitors should return the VISITOR sticker in exchange for his/her proof of identity at the end of their visit.

Visitors are only allowed on Cedefop premises when the visited person is clocked in.

Journalists are treated like external visitors. They must be announced like other visitors and present their proof of status (journalist's card). They must visibly wear their Visitors/journalist badge. If they visit Cedefop on their own initiative, access should be authorised by the Directorate or the Head of CID. and be accompanied by a staff member at all times.

Family members should register with the Security Guards. They will not be provided a badge nor do they need to have any ID. They should however signal when they are leaving the premises. Those family members who have children in the Day Care Centre (DCC) will receive special access cards which will allow them access to the DCC. In all other cases they are requested to register in the Security Booth.

Visitors who intend to see an exhibition are allowed to enter the premises only during the working hours of the reception desk assistants. They are requested to register at the Security Booth. In these cases, security is not required to keep a proof of personal identity. Exceptions are conferences or special events such as inaugurations or openings of exhibitions which are held outside the working hours of the reception desk assistants.

1.2.3 Visits by dignitaries or senior EU/Greek civil servants

The procedure for visits by dignitaries or senior EU or Greek civil servants is attached in Annex I.

1.2.4 Other EU institutions

Staff from other EU institutions wishing to visit Cedefop will be treated according to standard visitor procedures. In particular, they should:

- a) Present themselves, with proof of identity to the Security booth;
- b) Obtain, and visibly display, a temporary VISITOR sticker; alternatively they may use their service card;
- c) The Security Guard should arrange for the visitor to be met at reception.

1.2.5 Public exhibitions, receptions, meals, etc

An alphabetical list of names and functions of all external visitors must be provided (if possible) to the Security Officer before the event. The Security Officer will inform the guards of planned visits and of any additional security measures considered necessary.

The Security guard checks the name on the list and provides the visitors with badges (no identification needs to be kept at the security). If the name cannot be found, or no list is available at reception, the organiser of the meeting should be contacted for further advice.

Depending on the circumstances special security measures for these events will be agreed between the organiser and the Security Officer. These may differ from the procedures laid down hereafter and will be communicated to the Security guard prior to the event. They may include restrictions on the use of certain floors or areas in the Cedefop building.

1.2.6 Contractors and maintenance operatives holding a recognised “Contractors” card

The contractors and maintenance operatives must present themselves, with proof of identity and their contractor's card, at the Security booth. They must visibly display this card at all times when in the building.

1.2.7 Contractors and maintenance operatives who do not possess a recognised “Contractor” card

Some operatives from contractors, maintenance companies etc, may visit Cedefop only infrequently or irregularly. These operatives will not possess the regular “contractor card”, and should be processed as follows:

- a) they should present themselves, with proof of identity and written confirmation, eg. work order, request from Cedefop service etc, of their need to be present in the building, at the security booth;
- b) they should receive, and visibly display, a temporary CONTRACTOR sticker;
- c) the reception should contact the service that requested his/her presence, or for whom the work is being undertaken. Responsibility for the operative remains with the service that requested his/her presence, or for whom the work is being undertaken, at all times whilst in Cedefop;
- d) where operatives are seen to be leaving the building whilst wearing a CONTRACTOR sticker, they should be asked to surrender it for destruction.

In the event of an emergency visit outside working hours, the operative must:

- a) present him/herself to the Security booth, with details of the problem to be resolved and a copy of the work order, request from Cedefop service for the action required etc.;
- b) provide proof of identity, for retention by the Security guard at the Security booth whilst he is in the building;
- c) sign into the visitors' register and be issued with a temporary CONTRACTOR sticker;
- d) upon entry and exit to the premises, the equipment, toolboxes etc may undergo a physical search by the Security guard on duty;
- e) return the CONTRACTOR sticker to the Security guard on leaving the building, in exchange for his proof of identity.

II.1.3 Detection devices; forbidden items

It is forbidden to bring to Cedefop arms, explosives or other dangerous or poisonous substances which might pose a serious health risk.

Close protection teams for VIP's visiting Cedefop, members of the Greek government are exempt from this regulation after prior approval of the Security Coordinator.

All items carried by persons entering or exiting Cedefop buildings may be examined by the Security Officer and his or her delegates, where this is deemed necessary to maintain security. All persons entering or exiting Cedefop buildings must cooperate with the Security Officer and his or her delegates in these examinations.

If weapons, explosives or other dangerous substances illegally carried are detected, the authorities of the Host State may be informed.

II.1.4 Lock and Key management

There will be a key policy implemented in 2012.

II.1.5 Installation Security

Access to parts of the building holding vital installations such as the network nodes, the servers for Cedefop network and the IT back-up storage room is normally limited to designated Cedefop staff. Access by other people is only possible under the supervision of these persons. Transmitters or other electronic equipment compatible with the Directive 1999/5/EC are only allowed in these premises

II.1.6 Surveillance equipment

The Security Officer, subject to the specific approval by the Security Coordinator may, where this is considered necessary and appropriate in the interest of security, install video cameras or other surveillance equipment in specific areas or facilities. In such cases, Cedefop staff, external contractors and trainees regularly working in such areas or facilities must be informed about the installation and operation of such equipment.

II.1.7 Protection of vehicles and parking

Cedefop staff, external contractors and trainees who want to park their private vehicle in the parking space at Cedefop premises must provide details of their car registration to the Security Officer.

Depending on availability of parking space, staff and visitors may enter and park at Cedefop's premises. Cedefop is not liable for cars parked at the Centre. Owners park at their own risk.

Leaving cars in the premises during times of absence needs to be authorised by the Head of Resources and keys should be left with the guards.

Use of the parking facilities for Cedefop staff members is regulated in administrative circular No. 2008/1.

Taxis have access to Cedefop premises provided passengers are properly identified (as staff members or visitors who have received a badge).

CHAPTER II.2. — STAFF SECURITY

II.2.1. Security induction

The Security Officer briefs all Cedefop staff, external contractors and trainees on arrival at Cedefop, on their duties and obligations as laid down in this Cedefop security policy and in particular on the general obligation of discretion and confidentiality.

At the beginning of their contract or secondment to Cedefop, Cedefop staff (Officials, Temporary agents, contractual agents, trainees and Seconded National Experts) are asked by the Human Resources Service to sign a confidentiality declaration. At the end of the employment or secondment, all staff are asked by the HR service to sign a declaration regarding their continuing obligations under the Staff Regulations.

II.2.2. Training and authorisations

The Head of Area/Service instructs ICT to grant access to staff members under his/her responsibility on a need to know basis. Training will be provided if needed.

II.2.3. External contractors

The Security Officer must ensure that all persons performing specific tasks for Cedefop without being employed by the organisation perform the tasks with minimum risk to the security of Cedefop. Access to information by such persons is on a need-to-know basis.

All contracts Cedefop may conclude with companies employing such staff will include a clause on the necessary measures to safeguard the confidentiality of any classified information which may be obtained in the course of their duties. Where necessary, staff of those companies shall sign a confidentiality declaration.

CHAPTER II.3. — STAFF CONDUCT

The ICT User Policy defines the rules regarding the use of the ICT infrastructure, computers, telephones, etc. The ICT User Policy is available on the Intranet.

PART III: INFORMATION SECURITY

CHAPTER III.1. — Basic principles of information security

III.1.1. The need-to-know principle

Cedefop information may only be distributed or made accessible to persons who need to be acquainted with such information for the exercise of their duties.

III.1.2. Levels of protection of information security

The levels of protection of Cedefop information is a standardised format that indicates the protection measures to be applied to this information.

In this respect, two types of information can be identified:

Cedefop public information = information which is clearly recognisable as being public information. The decision to allocate the public status to information can only be taken by the Director or the Security Coordinator.

Cedefop confidential information = this level applies to information and material, the unauthorised disclosure of which could harm the essential interests of Cedefop, or of one or more Member States, or a concerned international organisation. Examples include information of a legal nature, selection and procurement data, health data and data collected by the confidential counsellors in the informal procedure.

CHAPTER III.3. — Handling of unclassified information

III.3.1. Creation, storage, dispatch, electronic transmission and destruction

Creation

There are no specific provisions regarding the creation of unclassified information. Documents containing unclassified information may be drafted and printed out on any workstation on Cedefop network.

Storage

Unclassified information in hard copies must be stored in locked offices or locked office furniture. Unclassified information can be stored in electronic form in the dedicated folder of the respective Area on the Cedefop network.

Internal dispatch and transmission

Dispatch refers to the sending of information in hard copy (via internal mail, postal services or delivery services).

Transmission refers to the sending of information in electronic form (via fax, e-mail, telephone, data, video, etc.).

With due regard to the 'need to know' principle, unclassified information may be dispatched via the internal mail system and sent electronically via Cedefop's electronic mail system.

External dispatch and transmission

Unclassified information may be transmitted by means of the communication links provided by Cedefop (e-mail, fax, telephone etc.). The ICT unit ensures that these communication links provide adequate protection against third party intrusion in order to meet the expectations of our partners with regard to the protection of unclassified information.

Destruction

Out of date and surplus copies of unclassified information, whether on paper or on any portable storage medium, should be destroyed (except when it would necessitate destroying equipment). Unclassified information in hard copies must be destroyed using the shredders available on Cedefop premises.

CHAPTER III.4. — Handling of Cedefop confidential information

Cedefop confidential information is subject to specific handling requirements.

III.4.1. Creation of Cedefop classified information

General

Documents containing information classified as 'Cedefop Confidential' must be marked as such at each page.

III.4.2. Printing

Documents classified as 'Cedefop Confidential' should only be printed using the 'secure print' function.

III.4.3. Reproduction

The security measures applicable to the original document must also be applicable to reproductions thereof.

III.4.4. Storage

Storage of hard copies or portable storage media

Information classified as 'Cedefop Confidential', whether on paper or on any portable storage medium, may only be stored in safe cupboards or locked cupboards.

III.4.5. Internal and external dispatch

CEDEFOP Confidential

Documents classified as 'Cedefop Confidential' must be dispatched:

- within Cedefop: in sealed envelopes with the classification level
- Outside Cedefop: in double-sealed envelopes. Only the inner envelope shall be marked with the appropriate classification level. The outer envelope shall bear a package number for receipting purposes. Receipts shall be returned to Cedefop.

III.4.6. Destruction

Documents classified as 'Cedefop Confidential' information, whether on paper or on any portable storage medium, can only be destroyed in line with the Cedefop retention schedule and the procedure for destruction of documents. Surplus copies must be shredded on Cedefop premises.

PART IV: PROVISIONS FOR ICT SECURITY

CHAPTER IV.1. — Introduction

For computer systems the main assets to be protected are systems and application configurations and, most of all, data. Relevant aspects associated with data involve: input/output, processing, storage and communications. Assets must be protected at all stages of the processing and at all times.

The purpose of the protection is to keep under control the following factors:

- Confidentiality
 - o Data access is limited to authenticated users owing pre-defined rights for the data asset in question.
- Integrity
 - o All system, application and data assets are operating correctly according to specification, in particular the data produced can be trusted.
- Availability
 - o Data output is delivered tot the point where it is needed.

The degree to which these factors are preserved provides a measure of the security of the system in place.

CHAPTER IV.2. — ICT security

Cedefop staff and external contractors who are given user accounts to use the ICT infrastructure are bound to the Security sections of the ICT User Policy.

User account passwords are subject to the password requirements of the ICT User Policy their passwords are subject to the password

PART V: PROCEDURES FOR DEALING WITH BREACH OF SECURITY

CHAPTER V.1. — What is a breach of security?

A breach of security occurs as a result of an act or omission contrary to a provision of the rules and principles laid out in the Security policy which might:

- endanger or compromise Cedefop information or affect its integrity and availability, including loss of information;
- pose a threat to installations housing Cedefop information, Cedefop premises or persons working at the premises.

Compromise of information occurs when it has wholly or in part fallen into the hands of unauthorised persons. This can be the result of negligence or indiscretion as well as intentional acts.

Threats to installations at Cedefop premises and to persons, means any act that might harm the persons working at or proper functioning of Cedefop.

CHAPTER V.2. — Responsibilities of the Security Officer

The Security Officer must take timely action in case of a security breach in order to establish the facts, assess and minimize the damage done, prevent a recurrence and notify the appropriate authorities of the effects of the breach of security.

CHAPTER V.3. — How to report a breach of security

All Cedefop staff, external contractors who have a reason to suspect that there has been a breach of security must report this to their direct superior and the Security Officer immediately. When detecting a possible breach of security outside Cedefop premises the Security Officer, in consultation with the Security Coordinator, can also report the security incident to the competent law enforcement authorities.

The same obligation applies if staff members have reason to believe that the security of Cedefop, their personal security or that of their colleagues or families has been, or may be threatened.

In cases where Cedefop confidential information is compromised – by theft or loss outside of Cedefop premises – the Security Officer must also report this to the Director.

Information relating to security incidents that have the potential to interfere with the security of Member States' networks will be reported to the appropriate national authorities as soon as possible.

CHAPTER V.4. — Investigations of breaches of security

Cedefop staff, external contractors and trainees must give all necessary assistance to the investigation of a security breach.

The results of the investigations are reported to the Security Coordinator and the Directorate.

Such reports should be stored in a separate file under the responsibility of the Security Coordinator, and kept for a minimum period of 10 years.

CHAPTER V.5. — Liability for breaches of security

All persons who are responsible for compromising Cedefop internal information or Cedefop confidential information, are liable to disciplinary action in accordance with the Staff Regulations, in particular the provisions laid out in Annex 9 of the Staff Regulations.



Christian Lettmayr

Acting Director

16/11/2012

Thessaloniki, 16.01.2012
RES/TBG/jk/2012/006**NOTE TO THE ATTENTION OF ALL STAFF**

Subject: Procedure for visits by dignitaries or senior European or Greek civil servants

1. Background

Cedefop has a legal and moral responsibility towards staff and visitors to its sites to ensure that their security and safety is adequately protected. This includes a duty to ensure that the required legislative and operational standards are met at all times. A failure to do so could open Cedefop to legal action or cause significant damage to its reputation or interrupt the smooth operation of the services.

Following a number of visits and in light of the experience gained, it has become evident that there is a need to establish procedures for the planning and operation of such visits so that Cedefop can meet its responsibilities.

2. Approach to be followed

In future, all visits, individual or in relation to conferences or events, by dignitaries or senior European or Greek civil servants will have to be notified to the Security Officer. The services organising such visits will have to fill in a safety and security form.

3. General points

Visits of dignitaries can be in relation to a conference/event organised at Cedefop or are specific for small meetings. Visits are usually announced or planned and in some exceptional cases can be unforeseen.

4. Procedure**4.1. Announced (planned) visits by dignitaries or senior EU/Greek civil servants**

Announced visits by dignitaries should be well organised to ensure the provisions of safety and security. A safety and security form has been established which will include all necessary information to organise such visits and also to assess the implementing provisions.

4.1.1. Organiser

The organisers have to fill in the safety and security form with the following information:

- a) Date of visit;
- b) Name(s) and title of visitor(s);
- c) In connection to event (if applicable);
- d) Purpose of visit – Host staff member (if applicable);
- e) Room to be used during the visit – If applicable tour of building, other areas;
- f) Duration of visit;
- g) the number of expected visitors;
- h) Details of organiser (Service, staff member to receive and escort the visitor);

The form has to be forwarded to the Security Officer as early as possible and not less than 14 working days before the actual visit. Any changes regarding or affecting the visit should be notified to the Security Officer immediately. The organisers have to respect the safety and security instructions given by the Security Officer.

4.1.2. Security Officer

- a) Contact the Local Police Authorities to announce the visit in writing; The Local Police Authorities will make the necessary arrangements according to the ceremonial protocol;
- b) Fills in a safety and security plan, if appropriate;
- c) Inform the Head of Resources on the planned visit and inform him of the preparations of the visit;
- d) Make the necessary arrangements for any additional security guards needed with the security company provider;
- e) Provide the security guards with instructions for the visit;
- f) Monitor the preparations for the visit ;
- g) Monitor the actual visit;

Any changes to or affecting these provisions of the security and safety plan must be notified and agreed by the Security Officer and Head of Resources.

4.2. Unforeseen (unexpected) visits by dignitaries or senior EU/Greek civil servants

Unforeseen visits by dignitaries or senior EU/Greek civil servants will be handled by the Security guards as for any other visitor.

4.2.1. Security Guards

- a) Ask the visitor to show an official identification document;
- b) Contact the staff member requested and inform about the visit;
- c) Contact the Security Officer and inform about the visit;
- d) If permission is granted, record the name of the visitor in the daily pass book and handover a visitor's badge;

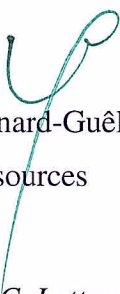
Visitors must wear their visitors badge visibly.

4.2.2. Recipient (Service or staff member)

- a) The person that is receiving the visitor should ensure that the visitor will be escorted at all times during the visit;
- b) Consult the Security Officer before visiting different areas of the building;

4.2.3. Security Officer

- a) Inform the Directorate and the Head of Resources of the visit;
- b) Follow up on any requests during the visit;
- c) Contact the affected services and the security guards;
- d) Report to the Head of Resources on the outcome of the visit;



Thierry Bernard-Guêlle
Head of Resources

c.c.: *Mr C. Lettmayr; Ms M. Brugia; Mr P. Descy;
Mr G. Bausewein; Ms A. Sainidou, All staff*

Attachment: Safety and Security form



SAFETY AND SECURITY FORM

(For visits by dignitaries or senior European or Greek civil servants)

Date of visit	
Name(s) and title of visitor(s)	
In connection to event (if applicable)	
Purpose of visit	
Host staff member (if applicable)	
Room to be used during the visit	
Please indicate if applicable (tour of building, other areas of building)	
Duration of visit	
Number of expected visitors	
ORGANISER:	
Area / Service	
Chief of Protocol (to receive/escort, etc)	G.O. Bausewein, Head of Area CID
Office nr	2.27
Tel. nr	288
Date and signature	

To be forwarded to the Security Officer