



COMMUNICATIONS *OFFICIELLES*

Les membres du personnel sont censés avoir pris connaissance des communications officielles ci-après.

La reproduction même partielle de ces informations par des personnes ou des institutions externes à l'Organisation exige l'approbation préalable de la Direction du CERN.

OFFICIAL NEWS

Members of the personnel shall be deemed to have taken note of the news under this heading.

Reproduction of all or part of this information by persons or institutions external to the Organization requires the prior approval of the CERN management.

ANNOUNCEMENT CONCERNING THE USE OF COMPUTERS AT CERN

After recent discussions in the Directorate the Director-General has approved revised Rules for the Use of Computing Facilities at CERN and a Procedure for the Investigation of Computer Security Incidents, which are published below.

J.J. Thresher
Director for Computing

REVISED RULES FOR THE USE OF COMPUTING FACILITIES AT CERN

13th March 1990

Introduction

The computing facilities at CERN, both in its Computer Centre and on the rest of its site, including mainframes, work stations, networks both on- and off-site, support services, program libraries, etc. are provided exclusively for the work of the Laboratory as set out in The Article II of the CERN basic Convention of the 1st July 1953, as amended 17th January 1971.

Almost all computers and workstations at CERN are connected directly or indirectly to a communication network. Hence mis-use or lack of adequate security on any of these systems can lead to problems for other systems at CERN. Furthermore for many of these systems, the maintenance support and the software licenses are provided under contracts made between CERN and their suppliers or other companies.

As a consequence these Rules including the above opening statement apply to all who make any use of computers, including work stations or personal computers, on the CERN site *unless* they are *not*

connected directly or indirectly to a communication network *and* are *not* subject to any contract or license agreement entered into by CERN.

The computing facilities at CERN are not available for public access and use: they are subject to specific rules as set out herein.

CERN reserves the right to: refuse registration and authorization to use any system that is its property; refuse permission to install a computer on the CERN site; disconnect any computer from the networks or exclude it from any contract, agreement or license between CERN and a third party.

Use in General

1. The computing facilities, including networks, must not be used other than for their intended purpose in connection with the CERN official programme of work, unless subject to a special agreement.

In particular, access to CERN's or third parties' computing facilities resulting in acts or omissions prejudicial to property and legitimate interests is strictly forbidden.

2. The operational procedures in force and the instructions of the staff in charge must be followed.

Account Codes, Passwords, Data and their Protection

1. Account codes and passwords must be used in a manner compatible with the official purpose for which they have been allocated.
2. A computer user shall take all reasonable care to protect his or her account and data from unauthorized access, in particular he/she should keep his/her password confidential and should not employ non-trivial passwords. He/she should follow the currently recommended methods for choosing a password (see CNL 197, 1989).
3. Any evidence of unauthorized access to an account or to data shall be reported immediately by the user concerned to the staff responsible.
4. A computer user shall not engage in unauthorized access to other accounts or the data of other users.
5. The search for the passwords of other users or system accounts, or any attempts to find and exploit any security weakness of computing facilities at CERN, or to make use of any of these facilities in attempts to attack computing facilities outside of CERN, are deemed to be abusive.
6. The confidential nature of any data or other material that may become available to a user, either in the normal course of his or her work, or inadvertently, shall be respected.

Privileged Use and Protection

1. Special services or arrangements and exceptional allocations of time or permanent file space must be requested from the staff appointed for that purpose.
2. When a computer user has been entrusted with a privileged account, it must be used only for the purpose for which it was intended; those privileges must not be abused.
3. For all users who have been given access to privileged use of a system, the level of their password protection must be increased appropriately.
4. If as a result of, for example, departure or change of project, a user no longer has the right to access privileged resources, then he or she must immediately inform the appropriate staff and return any material connected with that privilege.

Budgetary and Resource Control

1. A computer user must comply with the instructions in force or notified to him or her by the group or divisional administrator or other staff responsible for the control of resource usage.
2. He or she shall inform the appropriate administrative staff of any change in his or her status which would affect his or her eligibility for computer access, in particular departure or change of project.

Intellectual Property of the Organization and of External Holders

1. As CERN holds the intellectual property rights associated with its own computer hardware, software and documentation; neither a computer user nor any other person may reproduce them by any means, market them or make them otherwise publicly available, without obtaining the formal permission in advance from the Organization.
2. For certain CERN-written products the permission to reproduce is given by specific mention thereon.
3. The intellectual property rights of programs and associated material supplied by outside companies, are held externally. Such programs and material may only be used on those machines for which they are licensed and no unauthorized copies may be made for *use on-site or off-site*. Users may not reveal to a third party any information about such programs or material that would infringe on these property rights or about any security mechanisms incorporated in them.
4. In case of doubt, advice should be obtained from the Program Library office on questions of external property rights. If these rights are infringed through deliberate abuse or gross negligence, personal liability of the person involved may be involved according to the applicable laws.

Sanctions

1. In the case of duly established breach of one of the above rules or of any abuse of the computing facilities at CERN, the Organization may take action against the person concerned.

In the case of CERN Staff Members, the provisions for disciplinary measures of the CERN Staff Rules & Regulations will apply.

In the case of other persons, they would be subject to the authority of the Director General of CERN, who may take action ranging from a simple warning to immediate exclusion from further use of the CERN facilities.

2. In the case of acts and damage directed against CERN or its computing facilities, the Organization formally reserves all rights of civil and penal proceedings.

PROCEDURE FOR THE INVESTIGATION OF COMPUTER SECURITY INCIDENTS AT CERN

13th March 1990

Scope

This procedure should be followed when investigating any computer security incident once it is suspected that people are involved who are either Members of the CERN Personnel (see Staff Rules &

Regulations, January 1987, I 2.01) or any others working as part of, or in support of, the CERN official programme of work. Specifically, this includes personnel of companies providing equipment or services for the CERN Programme.

Aims

This procedure aims at:

1. Establishing as completely and as accurately as possible the details of any incident and its circumstances, as well as a first assessment of the damages caused to CERN, its personnel and its property.
2. Giving the individuals who appear to be involved the opportunity to state the facts from their point of view.
3. Establishing whether further action by the Organization is believed to be required and if this is the case preparing a detailed report.
4. Keeping the Management of CERN and any relevant external organizations informed.

Proposed Procedure

1. Security incidents are normally initially investigated by the technical experts responsible for the system(s) involved, in consultation with the Computer Security Coordinator (CSC) and with adequate information being given to the Chairman of the Computer Security Panel (CSP).
2. When it appears to them that it is likely that people working as a part of the CERN programme may have caused the incident, then the Chairman of the CSP should set up an *ad hoc* Board to investigate the incident.
3. The membership of this *ad hoc* Board should be as follows:
 - The CSC (Chairman).
 - The Experts involved.
 - In the case when either a Member of CERN Staff or a Visitor may be involved then:
 - a person nominated to represent the CERN Division Leader concerned.
 - The Group Leader or immediate supervisor of the person involved.
 - In the case of an individual from a company, a person nominated by that organization to represent it.
4. After a preliminary meeting to inform all members of the Board of the known details of the incident, the Board should start its investigations and meet with the person concerned and, if desired, one Member of the Personnel of his or her choice, to clarify further the technical details of the incident. At the same time the Board should listen to any statement of facts that the person involved may wish to present.
5. The Board should then:
 - a. Establish the facts and circumstances of the incident as soon as possible, whilst refraining from any judgment concerning responsibilities.
 - b. Evaluate if the seriousness of the incident requires further action by the Organization. In that case it should prepare a detailed report to be submitted to the Chairman of the CSP, who will then decide on the next steps, such as transmitting the report to the Division Leader(s), Director General and/or any companies or institutes concerned.
6. The above procedure has been presented, for simplicity, for the case where only one individual is involved. In the case where several people are concerned the membership of the Panel should include representatives of all Groups, Divisions or companies concerned.
7. In the interest of the security of the system(s) concerned and preserving evidence, the account(s) of the person(s) involved may be blocked for all or part of the above procedure.

General Guide-Line

The above procedure is intended to be as informal and as 'light' as possible. For many reasons in dealing with these security incidents, speed is of importance. However a reasonable balance has to be struck between the interests of the Organization and the rights of individuals.

VEHICULES IMMATRICULES EN FRANCE EN SERIE CONSULAIRE ET DIPLOMATIQUE

Les membres du personnel du CERN résidant en France et ayant droit à un véhicule immatriculé en série consulaire ou diplomatique sont informés que leurs conjoints titulaires de cartes de légitimation françaises AT, FI ou 'Assimilé à un membre de Mission diplomatique' peuvent conduire ce véhicule. Cette facilité ne s'applique pas aux enfants ni à d'autres personnes.

Il est rappelé par ailleurs qu'il n'est pas obligatoire d'équiper ce véhicule de phares jaunes.

Relation avec les Pays-Hôtes
Tél. 5152

DRIVING OF VEHICLES REGISTERED IN FRANCE WITH CONSULAR AND DIPLOMATIC LICENCE PLATES

Members of CERN personnel residing in France and having the right to a vehicle with consular or diplomatic plates are informed that it may be driven by their spouses provided they hold French identity documents of the AT, FI or 'Assimilé à un membre de Mission diplomatique' type. This privilege does not apply to their children or to other people.

It should also be noted that such vehicles are not required to have yellow headlights.

Relations with Host States
Tel. 5152

SEMINARS SEMINAIRES

Lundi 28 mai

SEMINAIRE AT-SU

à 11.00 h – Amphithéâtre LEP
bât. 30, 7e étage

**Géodésie, métrologie et topométrie
ou l'art de mesurer des objets démesurés**

par M. MAYOUD / CERN-AT/SU

Le géomètre moderne n'a plus grand chose de commun avec 'l'arpenteur' du proche passé. Plus encore, grâce aux techniques satellitaires, les géodésiens ou cartographes d'aujourd'hui ont pris beaucoup de hauteur par rapport au travail pénible des ingénieurs-géographes d'antan! Dans ces métiers, l'évolution technologique a été rapide et performante, répondant à des besoins variés, apportant des solutions méconnues, qui suscitent à leur tour des demandes nouvelles. Du génie civil à la robotique, en passant par la physique des particules, l'industrie, l'ingénierie et la recherche ont de plus en plus recours aux techniques de la métrologie géodésique. C'est en effet le seul moyen de mesurer précisément des objets de grande dimension, allant de la grosse pièce industrielle... à la terre elle-même.

Monday 28 May

CERN COLLOQUIUM

at 14.30 hrs – Auditorium

**The European Southern Observatory
its role in European astronomy : the very large
telescope project**

by H. VAN DER LAAN / Director-General
of ESO

This talk is prompted by the ESO exhibit in CERN's Microcosm. It will broadly sketch the two topics in the title. ESO is based on a convention, modelled after that of CERN, approved in 1962 and ratified in 1964. In its first 25 years ESO has evolved to assume a leading role in European astronomy, functioning as a research-service organization, a meeting place for exchange and collaborations as well as a centre for astronomy-technology, research and development. All three functions will be illustrated. In December 1987 the ESO council approved the proposal to build the 16-m equivalent very large telescope (VLT). This project, whose size is indicated by its aperture, its capital budget of around MDM 500 and the in-house plus community effort of around 1000 man-years, is