Computer Security Policy

and

Rules for users of the ECMWF computer systems

May 1995

Table of Contents

1. The requirement for computer security

Computer security protects the **availability**, **confidentiality** and **integrity** of the Centre's computer systems and the data held on these systems. In this context, "data" refers to information held in electronic form, such as software, meteorological records, text files, images, etc.

Availability ensures that forecast information and essential services are accessible to users when required.

Confidentiality measures protect sensitive or commercially valuable information against unauthorised access. ECMWF does not handle any classified information and has therefore no requirement for secrecy measures as employed at highly secure government installations. However, the current forecast results and the program codes of the forecast system have a significant commercial value and must be protected against unauthorised access. The Council of ECMWF has laid down precise rules governing the distribution of the Centre's products and software; such products and software must be protected against unauthorised access.

Integrity is required to safeguard the accuracy and completeness of the stored data. The integrity of the forecasting system and the meteorological archive is vital for the Centre's scientific and operational activities. The integrity of the operating systems in its own right is necessary to ensure availability and confidentiality.

With open, distributed systems and the growth of networks, computer security threats are becoming more widespread and increasingly complex. ECMWF's high speed computing facility is well known and may be perceived as an attractive target.

Intruders, commonly referred to as 'hackers', break into computer systems through external network connections. A malicious hacker gaining privileged access to one of the Centre's main computer systems could inflict serious damage, e.g. a prolonged period without operational service. Even an intruder without malicious intent represents a serious threat. The Centre's likely inability to identify the precise actions and intentions of any successful intruder will result in a loss of confidence in the integrity of the compromised systems. Substantial efforts would be required to remedy any such situation. Furthermore, any adverse publicity about the security of the Centre's computer systems would harm ECMWF's reputation. Incidents involving unauthorised access to the Centre's supercomputer could perhaps even jeopardise any export licenses required for future systems.

The program codes comprising the forecast system represent the Centre's most important asset. Unauthorised access to these codes could result in the loss of scientific advantages and could have an adverse impact on the relative quality of the Centre's forecasts, which are used commercially within many Member States.

Users, system administrators, and operators make errors which contribute directly or indirectly to security problems. Depending on the speed of notification, the damage caused can usually be contained and will not lead to any major incident. It is important that such errors are reported without delay to the relevant staff members. Any attempt by users, system administrators, or operators to conceal such errors would frequently make matters worse.

The objective of the Centre's computer security is to reduce to an acceptable level the risks posed by the various threats to both the Centre's computer systems and data.

2. Scope of the Computer Security Policy

This policy applies to all computer and data communications equipment installed at ECMWF. It deals with the access to these systems, the integrity and confidentiality of the data held on these systems and the availability of critical computing services.

The Computer Security Policy does not cover the physical security of the ECMWF site; this is the responsibility of the Centre's Administration Department.

3. Assets

The Centre's major data and computing assets include:

- the current analysis and forecast information;
- the meteorological archive;
- the program codes comprising the operational forecast system;
- the program codes developed by the Research Department;
- the program codes of tools and application packages developed at ECMWF;
- the computing and communication services required for the operational forecast runs and product dissemination.

4. Protected items

Data, systems, and equipment which are subject to security measures are classified as "protected data", "protected systems", and "protected equipment"; together they represent the Centre's "protected items". These are the Centre's major data and computing assets together with all other data, systems, and equipment which need to be protected to ensure that the objectives of this policy are met (e.g. operating

systems, configuration files, data communications equipment, personal systems connected to the Centre's local area network, banking and financial data, personnel data).

5. Threats

The possible threats to the Centre's data and computing assets are manifold. They vary in probability and in the seriousness of their consequences if carried out successfully. These threats can be classified as unauthorised access to systems, unauthorised access to data, destruction or modification of data, and denial of service.

Unauthorised access to systems:

- intruders breaking into the Centre's computer systems;
- trojan horses (disguised functions allowing access without proper authentication);
- use of the Centre's computing resources by anyone who is not an officially registered user of the Centre's computer systems;
- deliberate attempts to bypass the correct accounting of resources.

Unauthorised access to data:

- theft of the current forecast information;
- theft of the Centre's intellectual property (e.g. model codes);
- unauthorised disclosure of competitive information (to third parties);
- violation of license agreements;
- unauthorised disclosure of personnel information.

Destruction or modification of data:

- malicious codes (viruses, worms and other 'uninvited' software);
- human error and software malfunctions;
- intruders with malicious intent;
- disgruntled users;
- fraud initiated by staff targeting the Centre's financial system;
- environmental failures (fire, flood, power failures, etc.).

Denial of service:

- most of the threats listed above under the destruction or modification of data;
- attacks targeting the local or wide area network services.

6. Risk control strategy

The purpose of this policy and its managerial, technical, and operational controls is to reduce the risk to an acceptable level, while acknowledging that computer systems cannot be made fully secure . Thus the likelihood that a security threat is successfully carried out is minimised and the adverse impact of such an incident is reduced to an acceptable level.

The prevention of unauthorised access to the Centre's computer systems is given the highest priority. All external communication links must be well protected. This is particularly important for links to public networks (such as the Internet).

Next in priority will be the prevention of unauthorised access to data and the protection against threats posed by human error and environmental failures.

Lowest priority will be given to protection against wilful damage by 'insiders'. Such an attacker could potentially know all the security measures taken and how to circumvent them. The only defense lies in a strictly compartmentalised system to localize the damage. Complete security measures against such attacks would be too restrictive for the Centre's environment and risk control should therefore rely on other methods, such as screening of users and a reasonable compartmentalisation of the major information assets.

The controls laid down by this policy will be adapted in the light of new vulnerabilities or changing threats. The scientific nature of the Centre's work, and the resulting requirement for an open and easy exchange of information, must be taken into account whenever new security measures are implemented.

7. Network links to Member State sites

ECMWF has several hundred registered external users. These users work for meteorological institutions in the Member States and many of them require access to the Centre's most important computing asset, the high speed computing facility.

It is fundamental to the Centre's Computer Security Policy that the national weather services are responsible for the security at their end of network links to the Centre, and that the Centre's security measures can rely on identification and authentication information emanating from their sites.

8. Security Officer

The Centre has appointed a "Security Officer" who functions as the focal point for all matters related to computer security. The Security Officer ensures that the security measures implemented fit into an overall concept, coordinates the handling of major security incidents, liaises with the Member State Security Representatives, and provides advice on security matters and policy issues.

9. Prime Administrators

Each protected item will have a "Prime Administrator" who is responsible for the implementation and maintenance of the security measures appropriate for that protected item. Prime Administrators may delegate some of their tasks, but the responsibility will remain with them.

An inventory recording all protected items and their respective Prime Administrators will be maintained. The purpose of this "Inventory of Protected Items" is to ensure that the personal responsibilities for the implementation of the security measures are clearly assigned.

In the absence of an explicitly nominated Prime Administrator, the following assignment shall apply:

- for protected data: the staff member or consultant responsible for the area of work of which the relevant data is part;

- for protected systems and protected equipment: the staff member or consultant responsible for the configuration and administration of the relevant system or equipment.

10. Structure of the policy document

The ECMWF Computer Security Policy supersedes the "Computer Security at the European Centre for Medium-Range Weather Forecasts" document issued on 7 August 1990. The new policy comprises:

- the main document: "**Computer Security Policy**" (distributed to all registered users);

- Annex A: "**Rules for users of the ECMWF computer systems**" (distributed to all registered users);

- Annex B: "**Management controls within ECMWF**" (distributed within ECMWF only);
- Annex C: "**Operational and technical controls**" (distributed within ECMWF only).

All three annexes are an integral part of the policy.

These annexes will be supplemented by "Specific Guidelines" which will establish or clarify the Centre's policy in specific, limited areas.

ANNEX A

Rules for users of the ECMWF computer systems

A.1. Definitions

The "Centre's computer systems" are the computer systems installed at ECMWF.

A "user" is anyone accessing the Centre's computer systems.

A "user identifier" is a unique identifier issued to users by authorised Centre staff.

A.2. Use in general

The Centre's computer systems shall be used for tasks directly related to the Centre's program of work or for Member States' research only.

User identifiers are issued to users for their sole use and must not be made available for use by other persons. This is to ensure the accountability for the actions performed on each system.

Users must not access the Centre's computer systems using user identifiers other than those issued personally to them.[1)]

The confidential nature of any information that may become available to users, either in the normal cause of their work or inadvertently, shall be respected.

Users must not search for or exploit security weaknesses in the Centre's computer systems.

Users must not take any actions which could bring the Centre's name into disrepute; this applies in particular to the use of the Centre's network links to access services or computing facilities outside ECMWF.

A.3. Passwords and smart cards

Passwords and smart cards protect the Centre's computer systems against unauthorised access. Smart cards are personal access tokens and, like user identifiers, are issued to users for their sole use. The underlying authentication process is based on the physical possession of these cards; hence smart cards must be kept securely (similar to credit cards).

---

1) An exception to this is the use of the specific ECMWF utility designed to allow urgent work of absent users to be progressed.

Login passwords and the PIN numbers of smart cards must be kept confidential and must not be disclosed to other persons.

All users shall:

- employ non-trivial passwords and PIN numbers;
- change login passwords at least every month;
- follow the methods for choosing passwords as recommended from time to time;
- not re-use old passwords;
- safeguard smart cards issued to them against physical access by other persons;
- change passwords or PIN numbers whenever there is any indication that the passwords or PIN numbers have been compromised;
- report lost or stolen smart cards without delay.

Member State users should report lost or stolen cards to the relevant Member State Computing Representatives (or, if this is not possible, to the Call Desk at ECMWF). ECMWF internal users should contact the Call Desk.

A.4. Security awareness

Effective security requires the active co-operation of users. When using the Centre's computer systems, users must act in a security conscious manner.

Bad practices, such as including passwords in automatic login scripts or leaving active sessions unattended (without a software lock), should be avoided. Other users seen to follow any such bad practices should be encouraged to act in a more security-conscious manner.

A.5. Reporting of incidents

A security incident is any action that is in breach of the Centre's Computer Security Policy or any event that has, or could have, compromised the Centre's computer security. Security incidents must be reported as quickly as possible. Suitable reporting points are:

Security Officer	E-mail:	so@ecmwf.int
	Telephone:	+44 1734 499 000 (switchboard)
User Support	E-mail:	advisory@ecmwf.int
	Telephone:	+44 1734 499 801 (direct)

Call Desk	E-mail:	cdk@ecmwf.int
	Telephone:	+44 1734 499 303 (direct)

For incidents involving intruders, the use of electronic mail should be avoided. Successful intruders frequently monitor the electronic mail of a site they have broken into for signs that their presence has been discovered.

A.6. Reporting of security weaknesses

Users are required to report any observed or suspected security weaknesses in the Centre's computer systems without delay to the Security Officer.

A.7. Protection from malicious software

The Internet and other public sources offer a vast amount of free software. Software regarded as valuable for the Centre's programme of work may be imported, provided that the relevant guidelines effective from time to time are observed.

Software obtained for private use only should never be installed on any of the Centre's machines.

Any software for PC systems not acquired from an impeccable supplier must be checked by Computer Operations for embedded viruses prior to its installation.

A.8. Client/server applications

Server programs (executing on the Centre's computer systems) accessible to client programs outside ECMWF are potential security weaknesses. Such server programs must be explicitly approved by the Security Officer and the access control mechanism must be properly documented.

Users must not construct access paths to the Centre's computer systems which bypass the Centre's intended authentication mechanism.

A.9. Intellectual property rights

The intellectual property rights of programs and associated material supplied to ECMWF by vendors are normally held by these companies. Such programs and material may only be used on those machines for which they are licensed and no

unauthorised 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. This includes documentation supplied by vendors.

A.10. Updates and supplementary information

The currently valid version of the Computer Security Policy and any relevant Specific Guidelines are available in electronic form. Information on how to retrieve these documents can be found in the local help tool maintained by User Support.