ESA
Director General's Office

Distribution: all Staff.
ESA unclassified "releasable to the public"

ESA/ADMIN/IPOL(2015)7
Paris, 3 June 2015
(Original: English)

European Space Agency's IT Services User Policy

1. INTRODUCTION

The Agency's IT services[1] (hereinafter referred to as Agency-provided IT services) are provided to effectively support the operational needs of the Agency.

The usage made by physical or legal persons of Agency-provided IT services and of the information they contain shall be responsible, ethical and lawful at all times.

2. POLICY

The purpose of this instruction is to define the principles which govern the appropriate usage of Agency-provided IT services by physical or legal persons and this independent of their professional relation with the Agency and physical location.

3. SCOPE

The present policy applies to the usage made of :

i. Agency's IT services whether provided at corporate or programme/directorate level; and,

ii. IT devices neither owned nor provided by the Agency (e.g., the users' own IT devices) when such devices are used to access Agency's IT resources, services and applications.

[1] *IT services provided within the meaning of this policy are: workplace IT, network and mobility services, fixed and mobile telephony, video conference systems. The complete catalogue of IT services provided by the Department in charge of IT, and the process how to request and obtain these services can be found on the ESA IT Services Portal (esait.esa.int). Technical IT services provided by ESA programmes and directorates are also generally described by appropriate service catalogues that are made available to entitled users.*

4. PRINCIPLES

4.1 Protection of ESA IT assets

Users shall take at all time, including while on mission, at home or on leave, reasonable measures to ensure the physical protection and integrity of any ESA IT provided assets (computers, mobile telephones, etc.) in their custody. Such measures shall include damage from improper use, protection from theft and unauthorised modification or removal of data or equipment.

Any loss or damage shall be reported in accordance with the established policies on loss or damage to ESA assets, such policies being available on the Agency's internal portal.

4.2 Resource demand and usage

Users shall not place unreasonable or unwarranted demands upon the Agency's IT resources (e.g. network bandwidth, back-up storage, printers) the effects of which would impair the Agency's day-to-day operations and deny other users proper and unrestricted access to the services.

4.3 Personal Usage

Usage of the Agency's IT resources for personal purposes is authorised provided: it complies with the present policy, remains reasonable and does not affect the good name of the Agency, impairs its operations or legally exposes it. Examples of permitted personal usage are: online banking, travel bookings, private e-mail, web browsing, chat and access to social media.

4.4 Prohibited Usage

Any illegal or improper act which makes usage of Agency-provided IT resources is prohibited.

Such acts include, but are not limited to:

a) posting or transmitting messages, information, data, text, software, images or other material that is harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libellous, knowingly unlawful or otherwise objectionable or in contrast to the ESA Charter of Values and the Behavioural Guide;

b) violating another person's right of privacy;

c) impersonating any person or entity or otherwise misrepresenting your affiliation with a person or entity, including the unauthorised publication of opinions and notices that may be interpreted as those of the Agency;

d) knowingly posting, transmitting, reproducing, displaying or disseminating, without the right to do so any legally protected material or material that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party;

e) knowingly posting or transmitting any material that contains a virus or other form of 'malware';

f) knowingly compromising or attempting to compromise the security of any IT resource belonging to ESA or other organisations or individuals;

g) knowingly exploiting or attempting to exploit any security deficiency;

h) deleting any author attributions, legal notices, proprietary designations, trademarks or labels;

i) posting or transmitting any unsolicited advertising, promotional materials, 'junk mail', 'spam', 'chain letters', 'pyramid schemes' or any other form of private solicitation, commercial or otherwise;

j) unauthorised deletion or revision of any material belonging to another person or entity;

k) running a private business; and,

l) knowingly exposing ESA to security concerns, in particular related to information protection, communications security and protection of information technology.

4.5 Opportunity to filter access to web sites

The opportunity to restrict access to certain websites or categories of websites so as to protect the Agency's interests as well as that of its staff, is of the sole competence of the :

- Head of the Agency's Security Office if such access is of a nature to compromise the Agency's security's interest.
- Head(s) of the Department (s) in charge of IT services/systems for all other cases.

Internal and when appropriate external consultations shall be held prior to the decision being taken.

4.6 Communication of means of identification and authentication to third parties.

Where in order to prevent unauthorised access to the Agency's IT systems, users of such systems are provided with means of prior authentication (User ID, password...), they are not authorised to share and disclose such means to any third party including in the event of maintenance and upgrade.

Users shall act in accordance with the ESACERT password guidelines, in particular in case the password is lost, forgotten, or compromised.

4.7 Access to electronic files and e-mails

Users are recommended to log off from their computer or block access when leaving their work space.

Electronic files and e-mails on the Agency's IT infrastructure are deemed to be of professional nature and may – in compliance with the conditions defined hereunder – be accessed by the Agency at any time, in particular by a users' hierarchy if so justified by service requirements.

i) electronic files marked "Personal" or "Private" by a user, shall only be accessed in the presence of the concerned user unless :

- the latter refuses to be present after having being invited to do so. Such refusal shall be duly recorded in writing and reported to the persons identified under section 4.9 below; or,
- access is required by operational or security imperatives; or,
- access is requested by the Head of the Department in charge of personnel matters in the frame of on-going disciplinary proceedings.

ii) e-mails labelled "Personal" or "Private" or stored in an electronic file marked "Personal" or "Private" may only be accessed if so authorised

- by the user concerned; or,
- by the Head of the Department in charge of personnel matters in the frame of on-going disciplinary proceedings;
- by the Head of the Agency's Security Office for persons other than staff.

iii) e-mails not marked "Personal" or "Private" and not stored in an electronic file marked "Personal" or "Private" together with electronic files and e-mails not marked "Personal" or "Private", may, if justified by service requirements, be accessed at any time. Such access is authorised without any need for the user to be present or for the user's prior authorisation to be obtained. The user concerned shall always be informed about such access.

4.8 Monitoring of usage

The monitoring of the usage of Agency's IT resources and services will be done in an aggregated way, in compliance with the applicable Agency's rules on the processing of personal data and subject to the specific provisions established in the present instruction.

Individual usage will not be systematically tracked and recorded except in case of alleged abuse.

4.9 Disclosure of abuse and sanctions

In cases of averred or alleged abuse by a user, the Department(s) in charge of IT services/systems shall inform simultaneously:

- For ESA staff: the responsible hierarchical superior (Head of division/ department) and the head of the Department in charge of personnel matters;
- For all other users: the Head of the Agency's Department/service having the closest links with the concerned user (e.g. the initiating Department/service managing the relevant contract…) together with the user's direct employer.

Any usage of Agency-provided IT services averred contrary to the present instruction may give rise to appropriate legal, disciplinary or administrative actions.

5. IMPLEMENTING PROCEDURES

Implementing procedures, guidelines and best practices on appropriate use, personal devices, social networks, e-mail and web filtering are to be found on the Agency's IT Services Portal.

6. ROLES AND RESPONSIBILITIES

6.1 Where in the frame of contracts let by the Agency or other forms of agreements usage of Agency-provided IT services is to be made by non-ESA staff, the department in charge of managing the contracts or the agreements shall ensure that the said contracts or agreements contain the necessary provisions informing the other party(ies) of the present instruction and of any resulting sanctions in case of its breach.

6.2 The Agency's IT services or ESA programmes and directorates are responsible for ensuring that the present instruction is communicated to present users of Agency-provided IT services and to future users at the time such services are made available.

6.3 The Director in charge of corporate informatics is responsible for ensuring the overall implementation of this policy and its monitoring

7. SUPERSEDED ADMINISTRATIVE INSTRUCTIONS

This instruction revokes: ESA/ADMIN(97)19, ESA/ADMIN(98)16, rev.2, ESA/ADMIN(98)17, ESA/ADMIN(98)31, and ESA/ADMIN(2000)20.

8. ENTRY INTO FORCE AND VALIDITY

This instruction enters into force on the day of its publication and is effective for a period of four years subject to prior revocation or revision as determined by the Director General.

At least six months prior to the end of this period it shall be reviewed to establish whether it requires extension, modification or revocation.

9. PUBLICITY

The present instruction shall be communicated to all users of Agency-provided IT services.

Jean-Jacques Dordain
Director General