ESA
Director General's Office

Distribution: All Staff

ESA UNCLASSIFIED –
Releasable to the Public

ESA/ADMIN/IPOL-ITSW(2020)3
Paris, 17 September 2020
(Original: English)

ESA IT ACCEPTABLE USE POLICY

1. INTRODUCTION

The ESA Information Technology (IT) Services are provided to effectively support the operational needs of the ESA IT User community.

ESA IT Users are expected to comply with this instruction through responsible, ethical, and lawful behaviour, to ensure effectiveness of Information Security risk mitigation measures.

2. DEFINITIONS

Within the scope of this instruction, the following definitions apply:

Authentication is the provision of assurance that a claimed characteristic of an entity is correct.

Availability is the characteristic of being accessible and usable on demand by an authorised entity.

Confidentiality is the property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

ESACERT is the ESA Computer and Communication Emergency Response Team that coordinates the response to all Information Security incidents.

ESA Information is information owned by or entrusted to ESA.

ESA IT Users are ESA staff and any other person using ESA IT Services, irrespective of whether the person is working on or off-site.

ESA IT Services are operated by or on behalf of ESA to address the needs of ESA IT Users. These services include common productivity solutions (e.g., workplace, mobility, digital collaboration), business applications (e.g., enterprise resource planning), as well as domain-specific IT offerings under the responsibility of ESA programmes and directorates.

ESA Owned Device is equipment owned or otherwise possessed, for example leased, by ESA and assigned to ESA IT Users. This includes computers, mobile telephones, mass storage tools, etc.

Information Security is the preservation of Confidentiality, Integrity, and the Availability of information.

Integrity is the property of accuracy and completeness of information.

Rooting or **Jailbreaking** is the process of attaining privileged control over a device.

Shoulder Surfing is a technique used to obtain information such as personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder.

User Owned Device is equipment owned by ESA IT Users that is used for accessing ESA IT Services.

3. POLICY

The purpose of this instruction is to define the principles that govern the appropriate and secure usage of ESA IT Services, independently of the users' professional relation with ESA and their physical location.

The policy's objective is to provide adequate, suitable, and effective security of information owned by or entrusted to ESA.

4. SCOPE OF APPLICATION

The present instruction applies to all ESA IT Services, and their use.

The present instruction does not cover the management of IT elements that fall under common, corporate, and technical IT, including strategy, planning, procurement, development, and operations of IT. Specifically, when generated, operated, and funded under the Agency's programmes and activities, as well as third-party IT infrastructure. These IT elements are dealt with in the Policy for the Management of ESA's Information and Communication Technology.

5. PRINCIPLES

5.1 Protection of ESA Owned Devices

To prevent unauthorised access, alteration, or deletion of ESA Information, ESA Owned Devices are configured with defined security controls and digital identities. Altering this configuration puts Information Security at risk.

i. ESA IT Users of ESA Owned Devices shall take at all times, including while on mission, at home or on leave, reasonable measures to ensure the physical protection and Integrity of any ESA Owned Device provided to them and under their possession. Such measures shall include protection from damage due to improper use, protection from theft, and unauthorised access, disclosure, modification, or removal of data or parts.

ii. ESA IT Users of ESA Owned Devices shall refrain from performing any activity aimed at obtaining unauthorised privileges or impersonating other users, accounts, or services (e.g., Rooting).
iii. ESA IT Users of ESA Owned Devices shall refrain from disabling or reconfiguring security functions of such devices (e.g., encryption, antivirus, data loss prevention, monitoring agents).
iv. ESA IT Users of ESA Owned Devices shall refrain from removing, or altering, corporate installed software components, or configurations on such devices.
v. ESA IT Users of ESA Owned Devices shall permit the application of security patches, e.g., by regularly restarting the device.
vi. ESA IT Users shall refrain from sharing, lending, or leasing ESA Owned Devices to unauthorised third parties.
vii. ESA IT Users shall report any loss or damage to ESA Owned Devices in accordance with the ESA Security Directives.

5.2 *Protection of User Owned Devices accessing ESA IT Services and Information*

Permitting access to **selected** ESA IT Services through **selected** User Owned Devices for reasons of convenience, cost, or flexibility, requires a shared responsibility for Information Security. Permitting such access is at the discretion of the provider of the relevant ESA IT Service. ESA IT Users shall perform their best efforts to apply the protection measures described in Section 5.1 to their own devices.

In addition:

i. ESA IT Users of User Owned Devices shall enable available storage encryption systems;
ii. ESA IT Users of mobile User Owned Devices shall enrol their devices in ESA-provided device management services and comply with their terms;
iii. ESA IT Users shall remove ESA Information from User Owned Devices upon request.

5.3 *Reporting of security incidents related to ESA IT Services and ESA Information*

Not all cyber security incidents can be avoided through preventive measures. In order for ESA to be resilient to cyber-attacks, swift notification, and collaboration is essential.

ESA IT Users shall therefore promptly report any incident related to Information Security (e.g., suspect behaviour, information theft, unauthorised data modification, etc.) to the ESA Computer and Communication Emergency Response Team (ESACERT).

5.4 *Access, remote access, storage, and processing of ESA Information*

The effective end-to-end implementation of ESA’s rules for information classification, labelling, and handling as described in the ESA Security Directives relies on the active participation of each ESA IT User.

i. ESA IT Users shall limit storing ESA Information locally, i.e., on devices assigned to them, unless this is strictly necessary.
ii. ESA IT Services and ESA Information shall only be accessed through ESA networks or via authorised remote access mechanisms, unless approved for release to the public.

iii. ESA IT Users shall limit the use of ESA IT Services to defined admissible levels of information classification as defined in the ESA Security Directives.

iv. When sharing information via ESA IT Services, the ESA IT User shall actively manage the associated access rights, i.e., review and, as necessary, limit and remove access rights to ensure Confidentiality, privacy, and, to prevent accidental information leakage (e.g., by maintaining adequate access rights to files, folders, and database records).

v. ESA IT Users shall take the relevant provisions of:

   a. the Policy on ESA Records Management and Archives;
   b. the ESA Policy on Personal Data Protection; and,
   c. the ESA Security Directives

   into account when handling data (e.g., accessing, storing, processing).

5.5 Resource demand and usage

i. ESA IT Users shall refrain from placing unreasonable or unwarranted demands upon the ESA's IT resources (e.g., network bandwidth, back-up storage, printers, etc.), the effects of which would impair the ESA's day-to-day operations and deny other users proper and unrestricted access to the ESA IT Services.

5.6 *Personal usage*

Usage of the ESA's IT resources for personal, i.e., non-business, purposes is authorised, provided that the usage:

i. complies with the present policy;
ii. remains limited, reasonable, and appropriate;
iii. respects personal data protection in accordance with the ESA Policy on Personal Data Protection;
iv. does not negatively affect the reputation of ESA;
v. does not impair ESA's operations or legally expose ESA to avoidable risks.

Examples of permitted personal usage are: online banking, travel bookings, private e-mail, web browsing, chat, and access to social media.

5.7 Prohibited usage

Any illegal, inappropriate, or improper use of ESA IT Services and ESA resources is prohibited.

Such acts include, but are not limited to:

i. 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;
ii. violating another person's right of privacy;

iii. impersonating any person or entity or otherwise misrepresenting the affiliation with a person or entity, including the unauthorised publication of opinions and notices that may be interpreted as those of ESA;

iv. knowingly posting, transmitting, reproducing, displaying or disseminating or otherwise publishing, commercialising, or appropriating without the right to do so legally protected material or material that infringes any patent, trademark, trade secret, copyright or other intellectual proprietary rights of any person or entity;

v. knowingly posting or transmitting material that contains a virus or other form of malicious software;

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

vii. knowingly exploiting or attempting to exploit any security deficiency;

viii. deleting any author attributions, legal notices, proprietary designations, trademarks or labels;

ix. posting or transmitting any unsolicited advertising, promotional materials, spam e-mail, or any other form of private solicitation, commercial or otherwise;

x. unauthorised deletion or revision of any material belonging to another person or entity;

xi. running a private business;

xii. knowingly exposing ESA to security concerns, in particular related to Information Security, communications security and protection of information technology;

xiii. disclosing their Authentication credentials for ESA IT Services, e.g., memorised secrets or cryptographic keys, to any other party;

xiv. upon receiving Authentication credentials, not complying with the relevant, system-specific handling guidelines (see Section 8);

xv. processing ESA Information using unauthorised, or for personal-use, IT Services (e.g., unregulated cloud services, Software as a Service, personal e-mail).

ESA IT Users are made aware that ESA IT Services are subject to content-filtering and access limitations to potentially harmful internet resources.

5.8 Secure workplace

For effective end-to-end protection of information, working in a secure workplace environment is as important as having technical measures for information protection.

i. ESA IT Users shall prevent unauthorised access to ESA IT Services when leaving the workplace, even if only temporarily. Common measures include locking, signing off, or powering down devices that are used to access ESA IT Services.

ii. ESA IT Users shall only use computer peripherals, storage media, and accessories provided by ESA. If in doubt, ESA IT Users shall consult with the unit in charge of providing the relevant ESA IT Services.

iii. When teleworking or on mission travel, ESA IT Users shall ensure that Confidentiality appropriate to the ESA Information and ESA IT Services accessed can be established and maintained (e.g., using encrypted wireless networks, not using public or hotel computer terminals, prevent Shoulder Surfing).

5.9 Backup

i. ESA IT Users shall inform themselves of the backup service scope and any limitations to ensure effective backup operations.
ii. ESA IT Users shall use ESA IT Services for data backup. Other forms of backup of ESA Information shall not be used.

5.10 Access to electronic data

Electronic data (e.g., files and e-mails) stored or processed using ESA IT Services are generally deemed to be of professional nature and may, in general, be accessed by ESA at any time.

The following limitations apply:

i. Access to User Owned Devices is limited to data under device management (see 5.2);
ii. Electronic data marked "Personal" or "Private" may only be accessed under at least one of the following conditions:
   a. The ESA IT User concerned grants authorisation;
   b. Access is requested by the Head of ESA Internal Audit for the investigation of fraud as per ESA's Policy on the prevention, detection, and investigation of fraud;
   c. Access is requested by the ESA Security Office for the investigation and containment of Information Security incidents as per ESA's Security Directives;
   d. Access is requested by the Head of the Department in charge of personnel matters in the frame of on-going disciplinary proceedings as per ESA's Staff Regulations, Rules and Instructions;
   e. Access is requested to conduct criminal investigations by a governmental or jurisdictional authority of Member States, if authorised by ESA.

5.11 Service monitoring

ESA IT Services require monitoring to ensure service continuity as well as effective Information Security. Consequently, ESA IT Users shall, in particular, be aware that:

i. the monitoring of the usage of ESA's IT resources and ESA IT Services will be performed in compliance with the applicable ESA Policy on Personal Data Protection, and subject to the specific provisions established in the present instruction;
ii. individual usage will not be systematically assessed, unless required for security incident response or upon request as part of ESA's disciplinary process;
iii. ESA Owned Devices are subject to systematic and automated monitoring to ensure timely detection, prevention, and response to cyber threats.

6. ROLES AND RESPONSIBILITIES

This policy is applicable to all ESA programmes and ESA staff within their area of responsibility with the roles and responsibilities attributed as follows:

6.1 *The Department in charge of procurement*

The Department in charge of procurement is responsible for ensuring that this instruction is reflected in all contracts and agreements that involve ESA IT Users other than ESA staff members.

6.2 *The units in charge of providing ESA IT Services*

The unit(s) in charge of providing ESA IT Services are responsible for ensuring that the present instruction is communicated to current users of ESA IT Services and to future ESA IT Users at the time such services are made available.

6.3 *The Director in charge of corporate Information Technology*

The Director in charge of information technology is responsible for ensuring the overall implementation of this policy and its monitoring.

7. EVALUATION OF THE POLICY

The effectiveness of this instruction and its implementing documents will be evaluated by the unit in charge of corporate information technology on a periodic basis, or at any time upon the request of the Director General.

8. IMPLEMENTING DOCUMENTS

Specific implementing documents will be issued by the Department in charge of information technology as well as by ESA programmes and directorates that offer domain-specific IT. These documents shall be made available on the Agency’s intranet within the relevant IT service and information portals.

9. VALIDITY

This instruction is effective for a period of four (4) years subject to prior revocation or revision as determined by the Director General. At least six (6) months prior to the end of this period, it shall be reviewed to establish whether it requires extension, modification, or revocation.

10. SUPERSEDED INSTRUCTIONS

This instruction supersedes the European Space Agency’s IT Services User Policy (ESA/ADMIN/IPOL(2015)7), which is revoked.

11. ENTRY INTO FORCE

This instruction enters into force on the day of its publication.

12. PUBLICITY

The present instruction is made available to any ESA IT User using ESA IT Services, irrespective of whether the person is working on or off-site. Where ESA IT Users are not staff members, they must abide by the same principles detailed in this instruction when making use of ESA IT Services.

The Director General