Inter-American Institute for
Cooperation on Agriculture

Information and Communication Technologies Policy

September, 2021

Table of contents

I. Introduction

Addressing its commitment to improve and modernize administrative and technological processes to make rational, equitable and transparent use of resources, IICA has established the provisions contained in the present Policy, which is complemented with the procedures described in the Procedures Manual on Information and Communication Technologies.

The purpose of this document is to improve the efficiency, effectiveness and management of the Institute's technological services, guaranteeing appropriate, safe, confidential, integral, pertinent and respectful management of international regulations and standards in information and communication technologies, and in personal data protection.

To ensure compliance with the present Policy, the provisions and procedures have been grouped into three categories: security, users, and management of information technologies (IT).

II. Applicability and scope

This Policy is applicable to all IICA staff members and those people with access to the IICA technological platform, whether consultants, interns, associated personnel or staff from externally funded projects, in the Member States and at Headquarters, with which the Institute works to fulfill its mission.

III. Objective

To establish the guidelines and mechanisms for appropriate management of the IICA information and communications technologies platform.

IV. Definitions

1. Adware:

Malware that is usually embedded in the browser, though it could be elsewhere in the system, to place unwanted notifications on the device.

2. **Data center** (data processing center)

A large installation, construction or building that houses and maintains numerous electronic devices such as servers, fans, connections and other necessary resources used to maintain a network or system of computers, information, connections and data.

3. **Firewalls:**

A security device which is regularly used to segment the public world from the private world. A set of defined rules establish what traffic is permitted or prohibited and its direction.

4. **Hardware:**

Any physical component that is part of the information and communication technologies infrastructure, such as computer equipment, servers, switches, routers, access points, firewalls, storage devices such as SAN and NAS, video conference equipment, communications platforms and other related infrastructure.

5. **Host:**

Any connected device in a network, with capacity to request and provide information (data) with local (same network) or remote devices.

6. **Open System Interconnection (OSI)**

The International Organization for Standardization (ISO) has designed the Open System Interconnection (OSI) model which uses structured layers. The OSI model describes a structure with seven layers for network activities.

7. **Malware**

Any program that becomes installed in an operating system, whose purpose is to interfere with the correct functioning of the system.

8. **Phishing**

A cybercrime technique that uses fraud, deceit and deception to manipulate victims and get them to reveal confidential personal information.

9. **Roaming**

Capacity to send and receive calls over mobile networks outside of the local service area.

10. **Script**

A script directs a scene or sequence. In programming, the **script** contains written instructions in code that serve to execute diverse functions within a program.

11. Information system

IT application or tool that allows the user to enter, store, process and obtain information in an automated way.

12. Site

A website on the internet.

13. Software

Set of digital programs, instructions and IT rules to execute certain tasks on a computer.

14. Spam

Any form of unsolicited communication sent en masse (unsolicited mass email.) Spamming also exists through instant messages, text messages (SMS), social media and even voice messages. It is illegal to send spam.

15. Virus

Malware with the capacity to replicate, triggered by a user's action.

V. Institutional information technology provisions

Through the present Policy and Manual of information technologies procedures the Institute establishes the institutional provisions to ensure that the IICA information technology platform is managed safely, appropriately and in accordance with international standards.

1. Procurement and use of hardware and software

This Policy defines the guidelines for the definition and procurement of hardware and software in order to manage the growth of the Institute's technological architecture in an organized, logical and structured manner.

The Policy also provides the guidelines to be considered when procuring any software with a specific purpose for IICA, always guaranteeing that it meets the current regulations regarding licensing and procurement of goods and services.

When any software becomes critical for IICA operation processes and contains frameworking and/or custom-made developments, it becomes an Information System.

The determination of a technological structure that entails the procurement of hardware and software of an institutional nature shall be the responsibility of the Information and Communication Technologies and Digital Agriculture Division (GTIC-AD.) In the case of particular needs in the Delegations, the responsibility for this process is that of the Administrator along with the Representative, in coordination with the GTIC-AD. In both cases authorization is required from the Director of Corporate Services.

Procedures related to the procurement and use of hardware and software can be found in the Procedures Manual on Information Technologies.

2. Information Security:

IICA shall have the obligation to maintain the security of the information for which it is responsible, applying appropriate technical and organizational measures to guarantee a level of security in keeping with risk.

For this purpose a structure is established for the standardization, monitoring, control and improvement of the institutional information security system through an administrative structure based on best practices, in order to ensure the protection of information assets from unauthorized use, modification, damage or accidental or intentional destruction.

The appropriate definition of roles, permissions, access levels of IICA employees to different information systems, and to the IICA technological platform or physical IICA data centers, regarding support and information recovery mechanisms, contingency plans, data protection, etc., is intended to prevent information security incidents in the Institute.

2.1 Information security regulations:

2.1.1 IICA has a centralized team with high availability for the authentication and authorization of equipment (hosts) and users, for access to IT resources at Headquarters, for which remote access, wireless and wired platforms are used.

2.1.2 Physical access to the data center at Headquarters is gained through an access system for authorized staff only.

2.1.3 IICA has last generation perimeter security equipment to protect its local resources from external IT threats, and an exhaustive database of application signatures that use free use ports to send sensitive information.

2.1.4 IICA has an antivirus platform which includes a threat detection module.

2.1.5. Access to different IICA information systems undergoes a security process in different layers of the Open Systems Interconnection (OSI) model which, in combination with secure programming practices by developers provides greater protection of the information contained therein.

3. Use of institutional email

The institutional email service (iica.int) is an institutional tool available to staff members, interns, consultants and associated personnel for carrying out their work.

All institutional IT resources, including the use of email accounts, are subject to preventative maintenance and supervision mechanisms that guarantee the security and integrity of the Institute's technological platform.

3.1 Regulations for institutional email use

3.1.1. The institutional email service must be used strictly for the communication and processing of institutional activities. Messages and documents sent through this service are for all purposes of an official nature and therefore can be used to transmit approvals and authorizations or as means of proof. All staff members, interns, consultants and associated personnel have a personal password to operate the email account that they have been given, hence they have full responsibility for any email sent from their account.

3.1.2. The institutional email system applies filters and security mechanisms to prevent the entry of messages, files or links that may affect the integrity and security of the Institute's technological platform. To prevent these protection measures from deleting or blocking employees’ personal messages, personal communications must be handled through other email accounts.

3.1.3. Institutional email may not be used for the following actions:

a. Sending confidential information or information that is the exclusive property of the Institute to third parties not related to the Institute.

b. Sending emails that promote illegal or dishonest acts or acts against morality and good customs, which defame or damage the reputation of other people, which contain matters of an obscene or pornographic nature or which foster discrimination in any way (based on race, religious beliefs, nationality or gender.) Institutional email may also not be used for matters related to political parties or for electoral campaigns of any type.

c. Sending spam emails that contain viruses, email chains, phishing or any other characteristics that affect the security of the Institute's technological platform or which saturates the traffic of messages through it.

d. Sending to third parties a list of emails of Institute employees.

e. Sending messages to email address groups (e.g., gmundo.iica) that are not meant for collective attention or are not of mass interest.

f. Obtaining, sending or processing third-party personal data that does not comply with the provisions established in the Policy and Manual on said subject.

g. Where it is necessary to send files greater than 25 MB over email it is suggested that another type of mechanism be used.

3.1.4. Instant messaging programs (offered by the platforms Teams, Google, Skype and similar platforms authorized by the Institute) may be used by employees as a means of communication for work matters, hence their installation, updating and use is authorized on equipment that the Institute provides for staff members, interns, consultants and associated personnel, provided that they contribute to the efficient performance of institutional functions.

4. Use of institutional internet

The internet access or connection service is a set of hardware and software resources that are scarce and high-cost, hence the GTIC-AD is responsible for ensuring their proper use.

Increasingly accelerated technological development has increased demand for the use of this resource to address matters of personal, educational, investigative and professional interest. Because of this, administrating and prioritizing the use of this resource must be a constant and responsible task, as the internet channel through which information circulates between different Delegations, Units, Institutions and persons connected to IICA work is not always desired and a number of packets of information compete for it, some of which are useful to the Institute and others not.

4.1 Regulations for institutional internet use

4.1.1 The use of accounts and access codes in IICA computer browsers by persons different from the assigned user, with or without authorization of the user responsible, is prohibited.

4.1.2 The internet browser service is for the exclusive use of institutional activities.

4.1.3 The connection, disconnection or relocation of equipment within the IICA technological infrastructure without the authorization of the GTIC-AD is prohibited.

4.1.4 The use of P2P file sharing sites (such as Ares, eMule, Torrents, Limewire) is prohibited.

4.1.5 Pages that are visited using the internet service are subject to review by the GTIC-AD, which has been assigned as the division responsible for monitoring and preventing its use, and by the direct superior of each user.

4.1.6 Use, distribution or sharing of any program, script or command designed to interfere with the use, functionality or connectivity of any user, host, system or site on the internet (such as sharing via email messages containing viruses, control characters, etc.)

4.1.7 Configuring or defining a webpage to act in a malicious way against users who visit it.

4.1.8 Any activity related to the internet browser service is the sole responsibility of the user.

4.1.9 It is the responsibility of the user to protect the identity of their account and their password.

4.1.10 In making declarations or expressing personal opinions via the internet service, users must indicate clearly that these are of a personal nature and in no way reflect or represent those of IICA.

4.1.11 Access to websites or web pages that contain pornographic, racist, sexist material or any other material that degrades human beings; in the case of social media, blogs, commenting sites and file sharing sites that are catalogued as a threat, the GTIC-AD will block them by default through security measures. If for any reason the user wishes to visit these websites, they must request authorization for their access from the GTIC-AD with prior authorization from their immediate superior, and the user must duly justify that it is necessary for performing their institutional work.

4.1.12 Using the service in such a way that it constitutes a nuisance, abuse, risk or in any way threatens the integrity of internet service users.

4.1.13. Try to avoid or alter the processes or procedures of time measurement, use of broadband or any other method used by the GTIC-AD to register the use of products and services.

4.1.14. Violating the security of systems, sites or hosts without prior authorization from their owner.

4.1.15 Users are prohibited from interfering or trying to interfere with the services of any other user, host or network on the internet (denial of service attacks.) Examples of these prohibited activities include without limitation: (a) sending excessive amounts of data (such as saturating with any type of traffic that exceeds the acceptable norms in terms of size and/or frequency) with the intention of overloading systems, filling circuits and or making hosts crash; (b) trying to attack or disable a user, host or site; (c) use, distribution or sharing of any program, script or command designed to interfere with the use, functionality or connectivity of any user, host, system or site on the internet (such as sharing, via email messages containing viruses, control characters, etc.)

4.1.16 Changing identity information in order to impersonate another person or organization.

5. Use of mobile communication services

Mobile telephony has become a valuable instrument for promoting the development of organizations and strengthening communication processes to make them more efficient at global level.

As this is a form of technology that is constantly subject to a permanent, fast-paced transformation, it has become a resource of high institutional cost, both in terms of procurement and updating.

This Policy aims to establish guidelines to regulate the assignation and use of mobile phones, communication services (voice and data) that may be authorized to employees and the responsibility to make rational use of mobile telephony and assigned devices.

5.1 Regulations for use of mobile communication service

5.1.1 Mobile telephones must be procured in accordance with GTIC-AD technical guidelines and the stipulations in the Manual of procurement of goods and hiring of services, giving priority to the procurement of mobile devices through mobile telephony plans that guarantee the service required for the Institute at a lower cost.

5.1.2 The device to be procured must fulfill the technological requirements of the position for which it is to be assigned.

5.1.3 The hiring of additional services such as roaming, internet services and international telephony is limited to the necessity and relevance of the position.

5.1.4 Criteria for the assignation of mobile services and telephones:

a. Nature of the roles assigned to the position within the organizational structure that justify constant communication with relevant institutional bodies, or attention to emergency situations of the Institute.

b. For positions within the structure that are assigned institutional mobile telephone and service, both device and monthly consumption shall be defined by the Director General.

5.1.5. Criteria for the payment of monthly mobile services:

The Institute shall only cover payment for:

a. National telephone calls.

b. International telephone calls used for official functions.

c. Roaming services used during official travel.

d. Internet service where this is authorized.

5.1.6. It is important to encourage the use of the (secure) wireless Wi-Fi connection service and the use of collaboration and communication tools that reduce the use of roaming, such as Microsoft Teams, Open Scape (app for using conventional telephony on mobile devices), and any other technological option.

5.1.7. Responsibilities in the event of loss, due to misplacing or theft:

a. Cancel the mobile service immediately through the Administration in the case of Delegations, or through the Administrative Services Division in the case of Headquarters.

b. The employee must send a written explanation from their immediate manager, with a copy to Administrative Services Management at Headquarters and the Administration in the Delegations, indicating the circumstances in which the loss or robbery occurred.

5.1.8. The Administrative Services Division at Headquarters and the Administrators in the Delegations shall supply the employee to whom an institutional mobile telephone and service has been assigned with details of services and costs billed monthly by the provider for their review and checking.

6. Personal Data Protection Policy

The goal of this Policy is to guarantee the right of all people to see, update and rectify the personal data that has been collected on them in the databases or files that the Institute has compiled. For the purposes of the present Policy, IICA is responsible for processing this data.

The Policy shall be applicable to the personal data registered on any database that makes it subject to processing and which is in the power of the organization. Such processing shall be governed by the provisions in the Procedures Manual on Information Technologies; the Personal Data Protection Policy and its respective Procedures Manual on the protection of personal data.

VI. General considerations

Exceptions to the compliance of this Information Technologies Policy and the Procedures Manual on Information Technologies must be approved by the Director of Corporate Services. Furthermore, all exceptions to these regulatory instruments must be formally documented and registered by the Administrators in the Delegations and the GTIC-AD at Headquarters, where relevant.

VII. Responsibilities

Implementation of and compliance with the present Policy and Manual are the responsibility of all the members of the Institute and persons connected to the Institute who are authorized to access the IICA information and communication technology platform.

The Representatives and Administrators in the Delegations and the Director of Corporate Services at Headquarters shall ensure compliance with this Policy.

The guidelines contained in the present Policy must be implemented and fulfilled by the Administration of each of the IICA Delegations, even where, due to the size of operations, they do not have a staff member specializing in information and communication technology. At Headquarters, this responsibility falls to the Information and Communication Technologies and Digital Agriculture Division (GTIC-AD.)

Only those processes, procedures, systems that are of a corporate nature shall be administered directly by the GTIC-AD. In such cases, guidance and addressing of requirements shall come from said Division.

Internal auditing shall carry out reviews of the application and fulfillment of the present Policy and its Procedures, and shall provide their recommendations to the Director General and to the Director of Corporate Services.

VIII. Complaints

IICA has two means for receiving and addressing complaints, so that people can confidentially send and channel their reports or complaints regarding matters covered by the present Policy:

1. The official website: www.iica.int, section REPORTING/COMPLAINT; and,
2. The email address: ec.ce@iica.int.

All reports, complaints, investigations and information regarding the matter reported shall be examined and analyzed subjectively by the Institute's Ethics Committee, who shall establish their approach, disciplinary measures and corresponding actions.

IX. Publications

This Policy shall be available in the institutional repository, on the Institute website and on the institutional intranet.

X. Interpretation

Aspects not contained in the present Policy or which may lead to numerous interpretations shall be clarified by the Information and Communications Technology and Digital Agriculture Division, and authorized by the Director of Corporate Services.

XI. Review and adjustments

The Director of Corporate Services, or whomever they designate, shall be responsible for maintaining the content of this Policy up to date in accordance with relevant international standards and within the Institute's scope.

XII. Validity

This Policy shall come into force from the date of its notification by the Director General.