ICRISAT Policy Series

Information Security Policy

Version 1.0
Nov 2020

ICRISAT
INTERNATIONAL CROPS RESEARCH
INSTITUTE FOR THE SEMI-ARID TROPICS

Table of Contents

1. Version Control 2

2. Introduction 3

2.1. Objective....................3

2.2. Scope & Applicability....................3

2.3. Roles & Responsibilities....................3

2.4. Exceptions to the Policy 4

2.5. Frequency of Review 4

3. Policy Statement 5

3.1. Information Risk Assessment 5

3.2. IT Asset Management....................5

3.3. Information classification and privacy (including Personally Identifiable Information)......6

3.4. Business continuity management (Information security aspects)....................6

3.5. Information Security Incident Management....................6

3.6. Access Control 7

3.7. Physical & Environmental Security....................7

3.8. Operations Security 7

3.9. Communication Security 7

3.10. Third Party Information Security Management 7

3.11. Legal & Regulatory Compliance 8

3.12. Information Security Monitoring 8

4. Appendix....................9

4.1. Key Terms 9

4.2. Reference Documents/ links 9

1. Version Control

Policy Formulation:

Policy Category:	Governance
Policy Formulation date:	September 2020
Policy Approved by:	Governing Board
Policy Approval date:	1 Oct 2020
Policy Roll-out date:	1 Nov 2020
Policy Version:	1.0
Policy Owner:	Head ISU

Policy Amendments:

Date	Version	Changes made by	Changes approved by	Description of change

The Institute reserves the right to amend, suspend or rescind this policy at any time. While, the Institute has made best efforts to define detailed procedures for implementation of this policy, there may be occasions when certain matters are not addressed or there may be lack of clarity in the procedures. Such difficulties or lack of clarity will be resolved in line with the broad intent of the policy, by the Director General or Governing Board Chair (on case to case basis). The Institute may also establish further rules and procedures, from time to time, to give effect to the intent of this policy and further the objective of good corporate governance.

2. Introduction

The Information Security Policy (“Policy”) sets forth the principles for information security management reinforcing the Institute’s focus on delivering consistent, secure and timely IT Services to ICRISAT (“Institute”) users. It also describes the Institute’s framework to manage information security risks, ensuring compliance with applicable laws and ICRISAT’s policies, procedures, and guidelines.

2.1. Objective

The objectives of this Policy are as follows:

- To define general principles for information security management, ensuring high standards of confidentiality, integrity and availability
- To outline a framework where ICRISAT, with each user's cooperation, is able to protect the IT environment at the Institute and effectively manage external and internal risks applicable to the Institute’s IT systems and/ or associated assets
- To define broad roles & responsibilities of users and the Information Services Unit (ISU) with regard to information security management at the Institute
- To set the Institute's expectations for the delivery of consistently high-quality IT services based on user requirements
- To outline the related policies, procedures and guidelines which complement this Policy and are expected to aid the ISU and users in effective implementation of the framework defined in this Policy

2.2. Scope & Applicability

a) This Policy is applicable to all members of Institute’s workforce. This applicability does not depend on the physical work location of the member and extends beyond ICRISAT’s premises where they may potentially have access to the Institute’s information systems and associated assets.

b) This Policy covers the security of information systems and data networks owned or used by ICRISAT as well as the information that is stored, transmitted or processed by those systems.

2.3. Roles & Responsibilities

a) The Information Services Unit shall be responsible for:

- IT security management within the institute, acting as a central point of contact for IT security for both the workforce and external parties who are provided access to ICRISAT’s information system and associated assets
- Implementing controls and monitoring compliance under this Policy and related policies, procedures and guidelines
- Monitoring and responding to potential and/or actual IT security incidents
- Ensuring that the Institute’s workforce member is aware of his/her responsibilities related to IT system, IT assets, and information security management at ICRISAT

b) All members of the workforce are responsible for adherence to the provisions of this Policy and all related policies, procedures and guidelines, and must report any incident of misuse or abuse of information systems and associated assets of which they become aware as described in the relevant procedures formulated to support this Policy.

c) All external organizations which are provided access to the Institute's data or information systems must ensure compliance with the applicable Information Security policies, procedures and guidelines of the Institute

2.4. Exceptions to the Policy

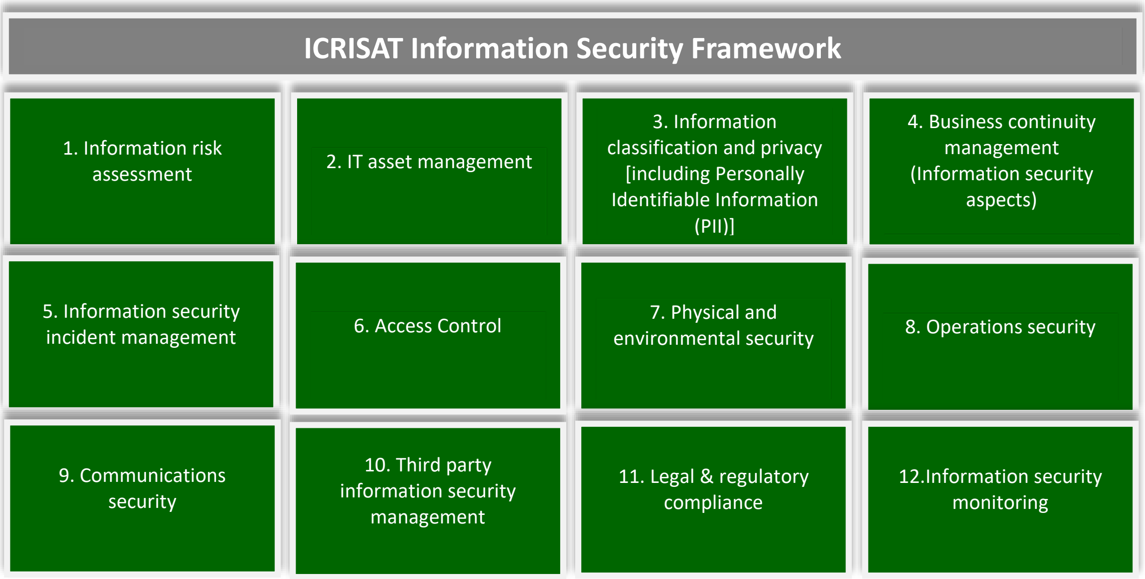
Any exception to this Policy shall require an approval from the Director General of the Institute and a post facto ratification shall also be obtained from the Governing Board at the next Board meeting. Any exceptions involving the Director General shall be approved by the Governing Board. The Policy Owner shall be informed of these exceptions and a record shall be maintained for monitoring purposes.

2.5. Frequency of Review

This policy shall be reviewed by the Policy Owner at least once in every 24 month period from the date of implementation or from the date of last review or earlier as directed by the Policy Council.

3. Policy Statement

ICRISAT's Information Security Framework is based on 12 pillars which form the foundation for effective IT governance at ICRISAT. Each of these pillars has a separate set of policies, procedures and/or guidelines, which when taken together form an integrated framework for information security at the Institute. The table below provides an overview of these components:



ICRISAT Information Security Framework			
1. Information risk assessment	2. IT asset management	3. Information classification and privacy [including Personally Identifiable Information (PII)]	4. Business continuity management (Information security aspects)
5. Information security incident management	6. Access Control	7. Physical and environmental security	8. Operations security
9. Communications security	10. Third party information security management	11. Legal & regulatory compliance	12.Information security monitoring

3.1. Information Risk Assessment

As part of the risk assessment exercise conducted at ICRISAT, the Institute deploys a risk-based approach to identify and understand the security risks and develop the risk mitigation plans; for which an appropriate risk assessment methodology must be selected and implemented to evaluate the operational impact and perform a threat and vulnerability analysis of all critical information technology assets (data, systems and processes) at the Institute.

In addition to the overall risk assessment exercise which incorporates all applicable risks at ICRISAT, periodic information risk assessments should be performed by the Information Services Unit (ISU) for critical IT processes, IT applications, information systems and networks at ICRISAT.

3.2. IT Asset Management

The Institute recognizes that its ability to safeguard IT assets (hardware and software) depends on robust IT asset management. The institute is committed to establish a structure for efficient and effective administration of its IT assets not limited to but encompassing the following:

- Maintaining the inventory of assets
- Issuance and re-issuance of assets
- Ownership and control of assets
- Defining lists of approved assets to be bought under IT asset class
- Acceptable use of assets

- Actions to be taken against any misuse or unauthorized use of assets
- Return and disposal of assets
- Loss or damage to assets

3.3. Information classification and privacy (including Personally Identifiable Information)

ICRISAT recognizes information collated and generated through the Institute's operations as a critical asset. Protecting these information assets is a key enabler to support high standards of IT governance at the Institute.

An information classification scheme is established by ICRISAT that applies throughout the Institute. The scheme takes into consideration the confidentiality of each piece of information, to determine the level of protection that should be applied to particular types of information, thereby reducing the likelihood of unauthorized disclosure or use of classified information.

Specifically, to manage information classified as Personally Identifiable Information (PII) through appropriate control mechanisms, the Institute has developed procedures based on the following principles:

- Collect personal data only if permitted by applicable law and after providing clear notice to the individual
- Specify the purpose for which personal data is being collected and use it for that purpose only
- Minimize the collection of personal data as needed for specified purpose
- Limit storage of personal data no longer than needed and have clear guidelines on personal data which needs to be collected across various functions/ processes
- Take safeguards to protect personal data against misuse or unauthorized use or disclosure

3.4. Business continuity management (Information security aspects)

The Institute is cognizant of the significance of information security continuity and aims to embed it as part of ICRISAT's Business Continuity Management (BCM) framework as outlined in the Business Continuity Management Policy. The key information security considerations for addressing BCM related risks at the Institute include:

- Planning information security continuity
- Implementing information security continuity
- Verifying, reviewing and evaluating information system continuity mechanisms
- Availability of adequate information processing facilities in the event of any disruption to the normal course of operations at the Institute

3.5. Information Security Incident Management

The Institute recognizes incident management as an important lever to respond to an unplanned event or service interruption and restore the affected IT services to their operational state. The Institute's *'Security Incident Management Procedure'* outlines the framework for detection, reporting and responding to security incidents.

3.6. Access Control

An integral part of maintaining high standards of information security governance at the Institute is to limit access to information processing systems/applications. The Institute has established access control rules, rights and restrictions to address information security risks and manage these within ICRISAT's risk appetite.

The key principles for access rights management at the Institute include:

- Security requirements of information systems/ applications should align with the information security framework defined at ICRISAT
- The Institute should clarify who needs to access and use the information residing within systems/ applications at ICRISAT
- Management of the access rights and privileged access rights including provisioning of access rights, maintaining the integrity of super users/ administrators controls, decommissioning access and performing periodic reviews of the access rights, audit logs across systems/ applications

3.7. Physical & Environmental Security

Physical and environmental security is the foundation of protecting the Institute from loss of connectivity and availability of computer and digital processing facilities caused by events including but not limited to theft, fire, flood, intentional destruction, unintentional damage, mechanical equipment failure, and power failures. Physical and environmental security measures institutionalized by ICRISAT should at all times be sufficient to deal with foreseeable threats and should be reviewed on a periodic basis for their effectiveness.

3.8. Operations Security

Operations security is a multi-faceted component of the information security framework of the Institute. The sub-components which should function cohesively to facilitate operations security at the Institute include:

- IT change management
- Software acquisition, development, licensing and maintenance
- Anti-virus/ malware protection
- Mobile and computing device security
- Back-up and restoration procedures

3.9. Communication Security

It is an obligation of the Institute to protect the integrity of its networks and the supporting information processing facilities as well as to maintain the safety, security and privileges of information transferred within the Institute and with any external parties.

3.10. Third Party Information Security Management

To maintain an agreed level of information security and curb the risk exposure within the risk appetite defined by the Institute, the Institute has developed an *'Information Security Policy for Third Party Relationships'.* The key aspects relevant to third party relationship management for ICRISAT are summarized below:

- Information security requirements for mitigating the risks associated with third party's access to the Institute's assets should be agreed and documented

- All relevant information security requirements should be established and agreed with each third party that may access, process, store, communicate, or provide IT infrastructure components for the Institute's information
- Regular monitoring, review and audit of third-party service delivery
- Changes to the provision of services by third party, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of information, systems and processes involved

3.11. Legal & Regulatory Compliance

Legal and regulatory compliances affecting information security should be identified, documented and given due consideration in decisions taken at the Institute (both strategic and operational). Further, a review of compliance with legal and regulatory requirements that affect information security should be performed on a period basis and as and when new legislations or regulatory requirements come into effect.

3.12. Information Security Monitoring

a) Appropriate security metrics and monitoring parameters must be developed and monitored on a periodic basis to ensure that the information security posture of the Institute is reviewed, and corrective action is taken, where necessary.

b) The information security status of IT processes, IT applications, information systems and networks at ICRISAT should be subject to thorough independent and periodic security audits to ensure that security controls have been implemented effectively and to provide the owners of targeted environments with an independent assessment of the security status of their respective environments. Such audits should be conducted at least on an annual basis.

4. Appendix

4.1. Key Terms

Term	Definition
Business continuity	Business continuity refers to risk management processes and procedures that aim to prevent interruptions to mission-critical services and re-establish or restore operations at the organization. This encompasses aspects related to information security continuity
IT incident	An unplanned interruption to an IT service or reduction in the quality of an IT service
Information security	Information security within the context of this policy refers to the preservation of confidentiality, integrity and availability of information assets at the Institute
Personally Identifiable Information (PII)	Personally identifiable information, or PII is any data that could potentially be used to identify a particular person. Examples include a full name, Social Security number, driver's license number, bank account number, passport number and email address
Targeted environments	Refer to critical IT processes, IT applications, information systems and networks at the Institute

4.2. Reference Documents/ links

Information Security Component	Reference documents
IT asset management	IT asset management policy
	IT acceptable use policy
Information classification and privacy [including Personally Identifiable Information (PII)]	Information classification and data privacy guidelines
	Data management procedures (research data)
	Data Management procedures (non-research data)
	PII management procedures
Business continuity management (Information security aspects)	Business continuity management policy
	Location specific BCM plans
Information Security Incident Management	Information security incident management procedures
Access Control	Access control procedures
Physical & Environmental Security	Workstation security guidelines
Operations Security	Software acquisition, development and maintenance procedures
	Change management guidelines
	Back-up & recovery procedures

	Cloud security procedures
	Mobile device security procedures
Communication Security	Network security procedures
	Server security procedures
	Email security guidelines
Third party information security management	Information security policy for third party relationships