



Republic of the Philippines  
Department of Transportation  
**PHILIPPINE RAILWAYS INSTITUTE**



**PRI Office Order No. 21, series of 2022**

**Policy and Protocols on the Use and Management of Information and  
Communication Technology Resources, Thereby Expanding the  
Technical Committee's Functions under PRI Office Order  
No. 12, s. 2022 and Repealing PRI Office Order No. 10, s. 2021**

**WHEREAS**, it is recognized under Article II of the 1987 Constitution that communications and information play a vital role in nation building, thus, harnessing the use of information and communication technology (ICT) is a catalyst towards national development, thereby spurring economic growth and ensuring transparent, efficient, and effective governance;

**WHEREAS**, the National E-Government Master Plan 2022 of the Department of Information and Communications Technology (DICT) states that the use of ICT in Government is seen as an enabler for nations to achieve digital transformation in the delivery of basic services;

**WHEREAS**, Executive Order (EO) No. 96, series of 2019, otherwise known as *"Establishing the Philippine Railways Institute under the Department of Transportation as the Planning, Implementing, and Regulatory Agency for Human Resources Development in the Railways Sector"*, created the Institute as a research and training center under the Department of Transportation (DOTr);

**WHEREAS**, the Institute shall serve as the planning, implementing, regulating, and administrative entity for the development of human resources in the railway sector, to ensure efficient, reliable, and safe railway transportation services;

**WHEREAS**, the Institute's core services such as training, certification and accreditation, and research and development, and its administrative and support services have been significantly delivered to both local and international stakeholders through the utilization of several digital productivity tools and communication platforms;

**WHEREAS**, the role and organizational impact of ICT is recognized in the realization of the Institute's mission and vision, thus, the need to establish rules and regulations on the use and management of its information and communication systems to ensure equitable, secure, and reliable access to these resources;

**NOW, THEREFORE, I, ANNELI R. LONTOC**, Officer-in-Charge – Executive Director (OIC – ED) of the Philippine Railways Institute (PRI), by virtue of the powers vested in

me, hereby order that the following rules and procedures be adopted:

## **ARTICLE I Objectives**

This policy intends to achieve the following objectives:

1. institutionalize the development and use of Information Systems Strategic Plan (ISSP);
2. designate the Technical Committee as the focal person for ICT resources and expand its functions;
3. establish standards and general policies on the use and management of ICT resources;
4. identify and report to appropriate authorities the prohibited actions in terms of utilizing ICT resources pursuant to existing laws, rules, and regulations;
5. maintain and protect privacy in accordance with the Data Privacy Act of 2012; and
6. provide a clear understanding on the policy direction of the Institute on ICT-related violations and its corresponding sanctions.

## **ARTICLE II Coverage**

This Office Order shall apply to the following:

- a. Users: All PRI personnel; and
- b. Components: The management of PRI-owned ICT facilities and resources including, but not limited to, online storage drive, equipment, software, accessories, networking facilities, and services.

However, it shall not apply to the management of electronic records as the latter shall be covered by the internal rules on document management.

## **ARTICLE III Definition of Terms**

Whenever used in this Order, the following terms shall have the respective meanings hereinafter set forth:

- a. Access – the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network;
- b. Alteration – the modification or change, in form or substance, of an existing computer data or program;

- c. Communication – refers to the transmission of information through ICT media, including voice, video, and other forms of data;
- d. Computer – refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks, and other devices connected to the internet;
- e. Cybersecurity – the collection of tools, policies, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user’s assets;
- f. Database – a representation of information, knowledge, facts, concepts, or instructions that are being prepared, processed, or stored or have been prepared, processed, or stored in a formalized manner and that are intended for use in a computer system;
- g. Email – also called electronic mail, is a means or system for transmitting messages electronically (as between computers on a network), messages sent and received electronically through an electronic mail system;
- h. Hardware – the electronic and physical components, boards, peripherals and equipment that make up a computer system as distinguished from the programs (software) that tell these components what to do; the physical component that consists of input devices, central processor, output devices and storage devices;
- i. Information and Communications Technology or ICT – totality of electronic means to access, create, collect, store, process, receive, transmit, present, and disseminate information;
- j. Information Systems Planner (IS Planner) – is designated by the Executive Director (ED) and shall be mainly responsible for the formulation, development, and implementation of an Information Systems Strategic Plan (ISSP).
- k. Information Systems Strategic Plan or ISSP – contains the agency’s overall strategy which involves medium term planning for its ICT thrusts, strategies and programs for development;
- l. Mailing List, Distribution List, or Group List – emails that need to be distributed and made accessible to a set of people are sent to the mailing list, distribution list, or group list, which will not have its own account inbox;

- m. Network – a group of two or more computer systems linked together. There are many types of computer networks, including: Local Area Network (LAN), which is a computer network limited to the immediate area, usually the same building or floor of a building, and Wide Area Network (WAN), which is meant to cover a wide geographic area, pertains to the physical network to all PRI offices nationwide;
- n. Operating System – a software that supervises and controls tasks on a computer. It directs a computer's operations, by controlling and scheduling the execution of other programs and managing storage and input/output processes;
- o. Software – a set of instructions to a computer to execute a command to process data. It is the non-physical component of a computer, which maybe an operating system, a development language, database management system, computer tools and utilities, or an application package, as well as the machine coded instructions that direct and control different hardware facilities;
- p. Spam – electronic junk mail or an unsolicited bulk email received that is unrelated to work and not otherwise justified; and
- q. User – refers to one or more of the following: (1) current workforce of the PRI; or (2) individuals connecting to a public information service. In addition, a user must be specifically authorized to use a particular ICT resource by DOTr and/or PRI.

#### ARTICLE IV

##### Information Systems Strategic Plan

Pursuant to the Office of the President's Memorandum Order No. 237, series of 1989 entitled "*Further Liberalizing The Existing Procedural Guidelines For The Acquisition And Use Of Information Technology Resources In Government*" and DBM-DOST-NEDA Joint Memorandum Circular No. 2014-01, regarding the *Government-Wide Medium-Term Information and Communications Technology Harmonization Initiative (MITHI)*, the Institute, through the Technical Committee (TC), shall formulate and implement its own Information Systems Strategic Plan (ISSP) to carefully outline and map out the modernization of its processes and facilities. The Information Systems Analyst (ISA) and Information Technology Officer (ITO) shall automatically be designated as members of the said committee.

The TC shall utilize the ISSP template, herein attached as **Annex A**, for the planning of the ICT resources that must be acquired the following fiscal year, conduct the annual inventory of existing ICT infrastructure, and submit the same to DOTr-Management Information Service (MIS), for onward transmittal to the Department of Information and Communications Technology (DICT), using the template provided by the latter. Thus, it shall be the due diligence of the IS Planner to disseminate the updated template and annexes.

## **ARTICLE V**

### **Information Systems Planner**

In view of the harmonization of PRI and national policies, the personnel responsible for the monitoring and implementation of this Order shall be the IS Planner required by the DICT. The IS Planner's main responsibility is the formulation, development, and implementation of the ISSP.

The primary IS Planner shall be the personnel occupying the ISA position, while the alternate shall be the personnel occupying the ITO position. The said planner shall be assisted by the TC, without the need of another Office Order.

In particular, the IS Planner shall have the following duties and responsibilities:

- a. develop the PRI's ISSP;
- b. coordinate with the DOTr-Management Information System, other relevant DOTr offices, and the DICT on all matters related to ICT;
- c. collaborate with all PRI divisions and sections, as well as with the PRI's designated Supply Officer, Budget Officer, and Procurement Officer to effectively execute its functions;
- d. perform all technical-related responsibilities during the conduct of the training courses pursuant to relevant PRI Office Orders;
- e. plan, implement, monitor, and evaluate the maintenance of ICT resources; and
- f. regularly monitor or check the quality or status of PRI-issued resources or devices.

## **ARTICLE VI**

### **Management of ICT Resources**

All ICT users shall abide by the acceptable usage policy of the Institute's ICT resources as follows:

#### **A. General Use of ICT Resources**

1. The use of official ICT resources (i.e., hardware, software, and other ICT-related machinery) must be limited to work-related activities and functions, and to authorized work-designated activities.
2. A user may only access the services and ICT resources that are consistent with his/her duties and responsibilities.
3. All ICT users are enjoined to cooperate by reporting suspected security breach, especially any damage to, or problems with their files, workstations, or other ICT equipment to the IS Planner through the ticketing system, if any, or through email in the absence of any other support system of the Institute.

4. Users are responsible for the daily operational upkeep and maintenance of their assigned ICT equipment. If there are technical problems that cannot be resolved by the user, it must be reported to the IS Planner through the ticketing system, if any, or through email in the absence of any other support system of the Institute.
5. In the absence of official laptops/computers, no office or job-related files shall be kept in the end-users' personal laptops/computers.
6. Users should not use personal, political, or religious pictures as their desktop wallpapers and screensavers. The IS Planner shall provide a standard desktop wallpaper for all PRI-issued laptops/computers to achieve an enterprise identity for the Institute.
7. The IS Planner shall periodically provide advisories to all users via email to keep them informed of the best practices to guard against existing cybersecurity threats and warnings regarding newly-discovered threats or any other material information.
8. The PRI Human Resource Team shall include in the newly-hired personnel's Onboarding Plan a discussion of this Order.

## **B. Implementing Procedures**

Operationalization of the management of resources including acquisition, maintenance procedures, and inspection activities of ICT resources shall be covered in a separate Manual, thus, changes thereto shall be governed by the PRI's relevant Office Orders on document management.

## **ARTICLE VII**

### **Prohibited Use of ICT Resources**

The following acts identified under Republic Act No. 10175, otherwise known as the "*Cybercrime Prevention Act of 2012*", are considered violations in the use of the Institute's ICT resources:

#### **A. Uses contrary to laws, customs, mores and ethical behavior**

1. Use of resources for criminal activities under the Revised Penal Code and other special penal laws;
2. Use of resources to commit computer-related offenses:
  - i. Computer-related forgery or the input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were

authentic, regardless whether or not the data is directly readable and intelligible; or the act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design;

- ii. Computer-related fraud or the unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent;
  - iii. Computer-related identity theft or the intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right; and
3. Use of copyrighted material including, but not limited to, the following acts:
- i. Copying, reproduction, dissemination, distribution, use, importation, removal, alteration, substitution, modification, storage, unloading, downloading, communication, publication or broadcasting of copyrighted material without permission;
  - ii. Infringement of intellectual property rights belonging to others through the use of telecommunications networks (*Criminal offense under Section 33(b) of the Electronic Commerce Act*);
  - iii. Copying a computer file that contains another person's work and submitting it for one's own credit, or, using it as a model for one's own work, without the permission of the owner or author of the work; and
  - iv. Submitting the shared file, or a modification thereof, as one's individual work, when the work is a collaborative work, or part of a larger project.

**B. Uses for personal benefit, commercial, or partisan activities**

- 1. Use of ICT resources for religious or political lobbying, for disseminating information or gathering support or contributions for social, political or cause oriented group, which are inconsistent with the activities of the Institute; and
- 2. Use of ICT resources to play games, or any activity unrelated or inappropriate to the duties and responsibilities of the personnel.

**C. Acts permitting other users for the unauthorized and/or to benefit personally from the use of the DOTr's ICT systems;**

**D. Acts that damage the integrity, reliability, confidentiality and efficiency of the ICT system:**

1. Unauthorized deletion, removal, modification, installation and/or destruction of any computer equipment, peripheral, operating system, disk partition, software, database or other component of the ICT System;
2. Attempt to crash, tie up, or deny any service on the ICT System, through acts such as, but not limited to, sending bulk mail, sending mail with very large attachments, and, sending data packets that serve to flood the network bandwidth without any valid purpose;
3. Concealment, deletion, or modification of data or records pertaining to access to the ICT System at the time of access, or alter system logs after such access for the purpose of concealing identity or to hide unauthorized use; and
4. Concealment of identity or masquerading as other users when accessing, sending, receiving processing or storing through or on the ICT System.

#### **E. Acts that encroach on the rights of other users**

1. Sending unsolicited mail such as chain letters, advertisements, jokes, trivia, announcements to non-official groups or activities, offers, inquiries, and the like (i.e., spamming);
2. Accessing, downloading, producing, disseminating, or displaying material that could be considered offensive, obscene, pornographic, racially abusive, culturally insensitive, or libelous in nature;
3. Sending messages which are fraudulent, maliciously harassing, obscene, threatening, or in violation of laws, administrative rules and regulations, or other policies of DOTr and the Institute; and
4. Interfering with or disrupting other computer users through acts such as, but not limited to, sending messages through pop-up screens, running programs that simulate trash, and running spyware to monitor activities of other users.

#### **F. Acts that violate privacy**

1. Hacking, Spying or Snooping:
  - i. Accessing, phishing, or attempting to gain access to archives or systems that contain, process, or transmit confidential information (authorized users should not exceed their approved levels of access, nor should they disclose confidential information to others);
  - ii. Decrypting, attempting to decrypt, or enabling others to decrypt such information which are intentionally encrypted, password-protected, or secured. Encrypted data are considered confidential, and include, but not limited to: passwords, digital keys and signatures;



- iii. Re-routing or capture of data transmitted over the ICT System; and
  - iv. Accessing, or attempting to access, restricted portions of the system, such as email lists, confidential files, password-protected files, or files that the user has no authorization to open or browse;
2. Unauthorized Disclosure:
- i. Copying, modification, dissemination, or use of confidential information such as, but not limited to, mailing lists and personal identifiable information of any sort without permission of the person or body entitled to give it;
  - ii. Searching, or providing copies of, or modifications to, files, programs, or passwords belonging to other users, without the permission of the owners of the said files, programs or passwords;
  - iii. Publication on mailing lists, bulletin boards, and the World Wide Web (www), or dissemination of prohibited materials over, or store such information on, the ICT System;
3. Prohibited materials under this provision include, but are not limited to, the following:
- i. Any collection of passwords, personal identification numbers (PINs), private digital certificates, credit card numbers, or other secure identification information;
  - ii. Any material that enables others to gain unauthorized access to a computer system. This may include instructions for gaining such access, computer or other devices.
  - iii. Any material that permits an unauthorized use-, who has gained access to system, to carry out any modification of the computer programs or data stored in the system; and
  - iv. Any material that incites or encourages others to carry out unauthorized access to or modification of a computer system.

## **ARTICLE VIII**

### **Enforcement and Sanction**

The IS Planner is designated to monitor compliance with this Order and report violations to the ED through its scheduled inspection and maintenance activities.

Attached to this Order is **Annex B** that shows the list of violations and equivalent administrative offenses and sanctions as provided by the DICT. Changes to the said list, as may be initiated by the DICT (proponent agency) or the Civil Service Commission (oversight agency) or the DOTr, shall automatically amend the said Annex without the need of amending this Order. ICT users who committed violation(s) therein shall be subjected to appropriate sanctions after formal hearing and fulfillment of due process. In cases where there is evidence of serious misconduct or criminal actions, appropriate charges shall be likewise filed to the proper authorities.

Specific procedures on the (1) acquisition and issuance of ICT resources; (2) access and storage of ICT Resources; and (3) management of ICT Resources are embodied in their respective Manuals (**Annex C**), as may be applicable. Additional manuals may be issued in the future to cover new ICT rules, protocols, and management systems as may be necessary to meet customer requirements and comply with future national ICT-related policies, following its internal rules on document management.

This Order conforms with the laws of the National Government. Thus, under some circumstances or as a result of investigations, subpoena, or lawsuits, the Institute may be required by law to provide electronic or other forms of information and/or records relating to the use of information resources.

## **ARTICLE IX**

### **Transitory Provisions**

The IS Planner shall conduct an orientation within thirty (30) working days upon this Order's effectivity to all PRI personnel. All personnel shall sign the Acknowledgement Form (**Annex D**) to signify that they: (a) truly understand the Order; (b) will fully comply with its provisions and its implementing procedures; and (c) are willing to be subjected to inspection and maintenance activities by the IS Planner.

Regarding electronic records, relevant PRI Office Orders and National Archives of the Philippines' (NAP) Memorandum Circular No. 210401, series of 2021 entitled "*Electronic Records Management Policy*," shall be complied with within one (1) year from the effectivity of this Order to complement the same.

## **ARTICLE X**

### **Amendments**

Amendment to any provision of this Order shall undergo legal review to ensure its compliance with the EO no. 96 s. 2019 and the IRR or DOTr DO No. 2020-005. This Order supplements PRI Office Order No. 12, s. 2022 and its subsequent amendments, effectively expanding the functions of the TC.

**ARTICLE XI**  
**Separability Clause**

If, for any reason, any section or provision of this Order is declared unconstitutional or invalid, the other sections or provisions hereof not affected by such declaration shall remain in full force and effect.

**ARTICLE XII**  
**Effectivity Clause**

This Order shall take effect immediately upon its issuance.

  
**ANNELI R. LONTOC, CESO I**  
Undersecretary, DOTr and <sup>pmb</sup>  
OIC-ED, PRI

PRI-AFS-F-ISP-YYYY-MM-XXXX-H



Republic of the Philippines  
DEPARTMENT OF TRANSPORTATION  
PHILIPPINE RAILWAYS INSTITUTE

INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

For the period \_\_\_\_\_ to \_\_\_\_\_

\_\_\_\_\_  
Name of Department/ Agency

PREPARED BY:

Signature \_\_\_\_\_  
Name in Print \_\_\_\_\_  
Position \_\_\_\_\_  
Tel. No. \_\_\_\_\_  
Fax No. \_\_\_\_\_  
E-mail Address \_\_\_\_\_

- SCOPE: ☐ ADMINISTRATIVE & FINANCE SECTION  
☐ CERTIFICATION & ACCREDITATION DIVISION  
☐ RESEARCH & DEVELOPMENT DIVISION  
☐ TRAINING DIVISION

APPROVED BY:

\_\_\_\_\_  
Name of Department/ Agency



PRI-AFS-F-ISP-YYYY-MM-XXXX-H

# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART I. ORGANIZATIONAL PROFILE

### A. DEPARTMENT/AGENCY VISION/MISSION STATEMENT

#### 1. MANDATE

- LEGAL BASIS
- FUNCTIONS

#### 2. VISION STATEMENT

#### 3. MISSION STATEMENT

#### 4. MAJOR FINAL OUTPUT

MFO 1:

MFO 2:

MFO 3:

### B. DEPARTMENT/AGENCY PROFILE



PRI-AFS-F-ISP-YYYY-MM-XXXX-H

# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART I. ORGANIZATIONAL PROFILE

1. Name of Designated IS Planner
  - Plantilla Position
  - Organizational Unit
  - E-mail Address
  - Contact Number/s
2. Current Annual ICT Budget
  - Other Sources of Funds
3. Organizational Structure
  - Total No. of Employees
  - No. of Regional/ Extension Offices (if any)
  - No. of Provincial Offices (if any)
  - No. of Other Offices (e.g. District, Field, etc.)

### C. THE DEPARTMENT/AGENCY AND ITS ENVIRONMENT (FUNCTIONAL INTERFACE CHART)

### D. PRESENT ICT SITUATION (STRATEGIC CHALLENGES)

### E. STRATEGIC CONCERNS FOR ICT USE (STRATEGIC CHALLENGES)

MAJOR FINAL OUTPUT	CRITICAL MANAGEMENT/ OPERATING/ BUSINESS SYSTEMS	PROBLEMS	INTENDED USE OF ICT



PRI-AFS-F-ISP-YYYY-MM-XXXX-H

# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART I. ORGANIZATIONAL PROFILE


## PART II. INFORMATION SYSTEMS STRATEGY

### A. CONCEPTUAL FRAMEWORK FOR INFORMATION SYSTEMS (DIAGRAM OF IS INTERFACE)

### B. DETAILED DESCRIPTION OF PROPOSED INFORMATION SYSTEMS

NAME OF INFORMATION SYSTEM/ SUB-SYSTEM	
DESCRIPTION	
STATUS	
DEVELOPMENT STRATEGY	



PRI-AFS-F-ISP-YYYY-MM-XXXX-H

# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART II. INFORMATION SYSTEMS STRATEGY

COMPUTING SCHEME		
USERS	INTERNAL	
	EXTERNAL	
SYSTEM OWNER		

### C. DATABASES REQUIRED

NAME OF DATABASE		
GENERAL CONTENTS/ DESCRIPTION		
STATUS		
INFORMATION SYSTEMS SERVED		
DATA ARCHIVING/ STORAGE MEDIA		
USERS	INTERNAL	
	EXTERNAL	
OWNER		





PRI-AFS-F-ISP-YYYY-MM-XXXX-H

# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART II. INFORMATION SYSTEMS STRATEGY

### D. NETWORK LAYOUT

## PART III. INTERNAL ICT PROJECTS

### A. INTERNAL ICT PROJECTS

1	NAME/TITLE		RANK:	
2	OBJECTIVES			
3	DURATION			
4	DELIVERABLES			

### B. CROSS-AGENCY ICT PROJECTS

1	NAME/TITLE		RANK:	
2	OBJECTIVES			
3	DURATION			
4	DELIVERABLES			
5	LEAD AGENCY			



PRI-AFS-F-ISP-YYYY-MM-XXXX-H

# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART III. INTERNAL ICT PROJECTS

6 IMPLEMENTING  
AGENCIES

### C. PERFORMANCE MEASUREMENT FRAMEWORK

HIERARCHY OF TARGETED RESULTS	OBJECTIVELY VERIFIABLE INDICATOR (OVI)	BASELINE DATA	TARGETS	DATA COLLECTION METHOD	RESPONSIBILITY TO COLLECT DATA
Intermediate Outcome					
Immediate Outcome					
Outputs					

## PART IV. RESOURCE REQUIREMENTS

### A. DEPLOYMENT OF ICT EQUIPMENT AND SERVICES

ITEM (Allotment Class/ Object of Expenditures)	Name of Office/ Organizational Units	Proposed Number of Units
---	---	--------------------------



PRI-AFS-F-ISP-YYYY-MM-XXXX-H

# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART IV. RESOURCE REQUIREMENTS

		YEAR 1	YEAR 2	YEAR 3
--	--	--------	--------	--------

### B. ICT ORGANIZATIONAL STRUCTURE

1. EXISTING ICT ORGANIZATIONAL STRUCTURE
2. PROPOSED ICT ORGANIZATIONAL STRUCTURE
3. PLACEMENT OF THE PROPOSED ICT ORGANIZATIONAL STRUCTURE IN THE AGENCY ORGANIZATIONAL CHART

## PART V. DEVELOPMENT AND INVESTMENT PROGRAM

### A. ICT PROJECTS IMPLEMENTATION SCHEDULE

NAME OF ICT PROJECT/S	Proposed Number of Units		
	YEAR 1	YEAR 2	YEAR 3

### B. INFORMATION SYSTEMS (IS) IMPLEMENTATION SCHEDULE

# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART V. DEVELOPMENT AND INVESTMENT PROGRAM

NAME OF ICT PROJECT/S	Proposed Number of Units		
	YEAR 1	YEAR 2	YEAR 3

### C. SUMMARY OF INVESTMENTS

ITEM (Allotment Class/ Object of Expenditure)	YEAR 1		YEAR 2		YEAR 3	
	PHYSICAL TARGETS	COST	PHYSICAL TARGETS	COST	PHYSICAL TARGETS	COST

### D. YEAR 1 COST BREAKDOWN

DETAILED COST ITEMS	OFFICE PRODUCT IVITY	INTERNAL ICT PROJECT 1	INTERNAL ICT PROJECT 2	CROSS- AGENCY PROJECT 1	CROSS- AGENCY PROJECT 2	CONTINUING COSTS

### E. YEAR 2 COST BREAKDOWN

DETAILED COST ITEMS	OFFICE PRODUCT IVITY	INTERNAL ICT PROJECT 1	INTERNAL ICT PROJECT 2	CROSS- AGENCY PROJECT 1	CROSS- AGENCY PROJECT 2	CONTINUING COSTS



# INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

## PART V. DEVELOPMENT AND INVESTMENT PROGRAM

--	--	--	--	--	--	--

### F. YEAR 3 COST BREAKDOWN

DETAILED COST ITEMS	OFFICE PRODUCT IVITY	INTERNAL ICT PROJECT 1	INTERNAL ICT PROJECT 2	CROSS- AGENCY PROJECT 1	CROSS- AGENCY PROJECT 2	CONTINUING COSTS



Republic of the Philippines  
**DEPARTMENT OF TRANSPORTATION**

**ANNEX B<sup>1</sup>**

**VIOLATIONS AND EQUIVALENT ADMINISTRATIVE OFFENSES AND SANCTIONS**

<b>VIOLATIONS</b>	<b>EQUIVALENT ADMINISTRATIVE OFFENSE</b>
Commercial Use - Use of Agency ICT Resources for commercial purposes and product advertisement for personal profit	Dishonesty / Grave Misconduct
Religious Lobbying - Use of Agency ICT Resources for religious lobbying	Conduct Prejudicial to the Best Interest of the Service
Political Lobbying - use of Agency ICT Resources for political lobbying	Engaging directly or indirectly in partisan political activities by one holding non-political office
Copyright Infringement - Reproduction, duplication or transmission of copyrighted materials	Dishonesty
Criminal Use - Using the resources for criminal activities	Grave Misconduct
Stealing - stealing information resources both hardware or software or any part of the network resource	Grave Misconduct
Concealing Access - concealing one's identity or masquerading as another user to access the information resource, send/receive, process, modify or store data on the Agency ICT Resources	Grave Misconduct
Password Disclosure - disclosure of user password protected account or making the account available to others without the permission of the E-mail System Administrator	Grave Misconduct
Unlawful Messages - use of electronic communication facilities (such as e-mail,	Simple Misconduct

<sup>1</sup> Department of Information and Communications Technology (DICT) Memorandum Circular No.: 2015-002, entitled [\*"Prescribing the GovMail Service Guidelines for Philippine Government Agencies"\*](#), pp. 25-27


talk, chat or systems with similar functions) to send fraudulent, harassing, obscene, threatening or other offensive messages	
Offensive Prohibited Materials - use of computers, printers, electronic mail, data network and other related resources to produce, disseminate, store or display materials which could be considered offensive, pornographic, racially abusive, libelous or violent in nature	Simple Misconduct
Prohibited Materials - using or encouraging the use of materials that includes instructions to gain unauthorized access (e.g., Hacker's Guide)	Simple Misconduct
Unauthorized reading of e-mail or private communications of other users, unless otherwise requested to do so by said user	Simple Misconduct
Misrepresentation in sending e-mail messages	Falsification of official document or Simple Misconduct
Not cooperating with any investigative process in line with computer, network or system abuse	Violation of Reasonable Rules and Regulations
Disclosure of Agency Confidential Information - transmission of information without authority and/or proper security clearance	Disclosing or misusing confidential or classified information officially known to him/her by reason of his/her office and not available to the public, to further his/her private interests or give undue advantage to anyone or to prejudice the public interest
Access to lewd sites and/ or materials - a user shall not view, transmit, retrieve, save or print any electronic file, image or text which may be deemed sexually explicit or pornographic	Violation of Reasonable Rules and Regulations

## ADMINISTRATIVE OFFENSES AND SANCTIONS

(Based on the CSC Uniform Rules on Administrative Cases in the Civil Service)

OFFENSE	SANCTIONS
Engaging directly or indirectly in partisan political activities by one holding non-political office	1st Offense - Dismissal
Falsification of official document	1st Offense - Dismissal
Grave Misconduct	1st Offense - Dismissal
Dishonesty	1st Offense - Dismissal
Disclosing or misusing confidential or classified information officially known to him by reason of his office and not available to the public, to further his private interests or give undue advantage to anyone or to prejudice the public interest	1st Offense - Suspension for six (6) months and one (1) day to one (1) year 2nd Offense - Dismissal
Conduct Prejudicial to the Best Interest of the Service	1st Offense - Suspension for six ( 6) months and one (1) day to one (1) year 2nd Offense - Dismissal
Simple Misconduct	1st Offense - Suspension for one (1) month and one (1) day to six (6) months 2nd Offense - Dismissal
Violation of existing Civil Service law and rules of serious nature	1st Offense - Suspension for one ( 1) month and one (1) day to six (6) months 2nd Offense - Dismissal
Violation of Reasonable Office Rules and Regulations	1st Offense - Reprimand 2nd Offense - Suspension for one ( 1) to thirty (30) days 3rd Offense - Dismissal



	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Acquisition and Issuance of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-AII-000
		EFFECTIVITY DATE:	SEP 09 2022
		REVISION NO.:	00
		PAGE NO.:	Page 1 out of 9

DOTr - PRI  
 MASTER COPY

Control No.: PRI-AII-000  
 Signature: 

## I. OBJECTIVE

The industrial revolution led to the acquisition of various Information and Communication Technology (ICT) resources to meet the increasing volume of government transactions and persisting demand for efficient and effective delivery of public service. With the declaration and transition to the new normal, this has become more evident, thus, the need to establish guidelines governing the acquisition and issuance of IT resources in the Philippine Railways Institute (PRI).

## II. SCOPE

This Manual shall generally cover the general architecture of PRI information systems, general acquisition and issuance protocols including budgeting and accounting rules on ICT resources.


Specifically, this Manual shall provide a working procedure for the following:

- a. Request for ICT Resource;
- b. ICT Inventory Management Procedure;
- c. Preparation of Triennial Information Systems Strategic Plan (ISSP); and
- d. Amendment to the Triennial ISSP.

## III. DEFINITION OF TERMS

Whenever used in this Manual, the following terms shall have the respective meanings hereinafter set forth:

TERM	DEFINITION
<i>Architecture</i>	: May refer to either hardware or software, or to a combination of both which defines a system's broad outlines and precise mechanisms to function.
<i>ICT Solutions</i>	: The various ICT technologies that are currently existing or will be proposed to run the information systems. Examples of ICT solutions are: for Network – Virtual Private Network, Thin Client; Wireless; for Security – Firewall, Public Key Infrastructure (PKI); for Storage – Storage Attached Network (SAN), Imaging, Warehousing; for Data Capture – Biometrics, Finger Scan, Optical Scan, Optical Mark Reader (OMR), Optical Character Recognition (OCR).
<i>Information System (IS)</i>	: A system of major processes or operations which facilitates the storage, processing, retrieval and generation of information for decision making, planning, controlling and monitoring purposes. It also refers to a group of related processes (manual or computerized)

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Acquisition and Issuance of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-AII-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 2 out of 9


TERM	DEFINITION
	designed to generate information for the exclusive support of a major functional area of an organization (e.g. Personnel Management Information System, Logistics Management Information System, Financial Management Information System, etc.).

IV. REFERENCE DOCUMENTS

- a. Commission on Audit’s (COA) Circular No. 97-003, entitled “Accounting Guidelines on the Acquisition, Maintenance and Disposition of Information Technology Resources”
- b. Department of Information and Communications Technology (DICT) No. 2020-010, entitled “Amendments to Department of Circular No. 2017-002 Re: Prescribing the Philippine Government’s Cloud First Policy”
- c. DICT No. 2017-002, entitled “Prescribing the Philippine Government’s Cloud First Policy”
- d. ISO 9001:2015 Standard - Quality Management Systems, specifically Clause 7.1.3 Infrastructure - (d) information and communication technology which mandates organizations to determine, provide, and maintain the infrastructure necessary for the operation of its processes and to achieve conformity of products and services.
- e. DBM-DOST-NEDA JOINT Memorandum Circular No. 2014-01, entitled “ICT Plan and Budget for FY 2015: Government-Wide Medium-Term Information and Communications Technology Harmonization Initiative (MITHI)”
- f. Office of the President’s Memorandum Order No. 237, s. 1989, entitled “Further Liberalizing the Existing Procedural Guidelines for the Acquisition and Use of Information Technology Resources in Government”

V. GENERAL ARCHITECTURE OF PRI INFORMATION SYSTEMS


- a. Attached as [Annex A](#) is the general architecture of all information systems showing the PRI’s subsystems, linkages, sources of data, or databases.
- b. The framework exhibits the interoperability of the PRI’s processes and illustrates the various data and information that flows and is being exchanged internally within the office and externally to stakeholders or relevant interested parties.
- c. The purpose of the framework is to identify the data and relationships of information that are essential components when developing or procuring hardware,

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Acquisition and Issuance of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-AII-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 3 out of 9

software, or cloud-computing platforms from open sources or third-party service providers, as well as in deciding the infrastructure and the pertinent ICT resources that may be acquired.

## VI. GENERAL ACQUISITION PROTOCOLS AND ACCESS POLICY

- a. To maximize office productivity, it shall be strived by the PRI to have a 1:1 Computer/Laptop to Employee ratio.
- b. In terms of ICT-related acquisition concerns, requests shall be submitted through a ticketing system, or in absence thereof, through email to serve as verifiable evidence of request.
- c. Network:
  - 1. A structured local area network has been established by the Department of Transportation (DOTr) - Management Information Service (MIS) for all users to provide optimal network connectivity.
  - 2. Secure Wireless Network Services are made available by the DOTr - MIS in designated areas within the Institute’s premises to provide wireless network access to users. It is the responsibility of the user not to disclose the password to other users to prevent security issues arising from unauthorized access.
  - 3. In the event of office transfer, structured cable management may be undertaken by the IS Planner or may be outsourced, whichever is deemed more efficient.
  - 4. Access to the internet within the Institute’s premises may be without any filtering system to promote creativity within the workplace. Nonetheless, the ED may subsequently issue advisories on the use of internet filtering systems (i.e., some websites may be blocked like Facebook, Youtube, etc.).
- d. The default homepage of all officially-issued computers or laptops shall be the Institute’s website. In the absence of the Institute’s website, it shall be the DOTr website.
- e. The acquisition of software or online platforms shall follow the DICT’s *Cloud First policy*.
- f. The IS Planner, through the ED, shall issue an advisory indicating the date and required participation of concerned personnel for the conduct of semestral maintenance and inspection of the PRI’s ICT resources.

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Acquisition and Issuance of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-AII-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 4 out of 9

**VII. BUDGETING AND ACCOUNTING RULES**

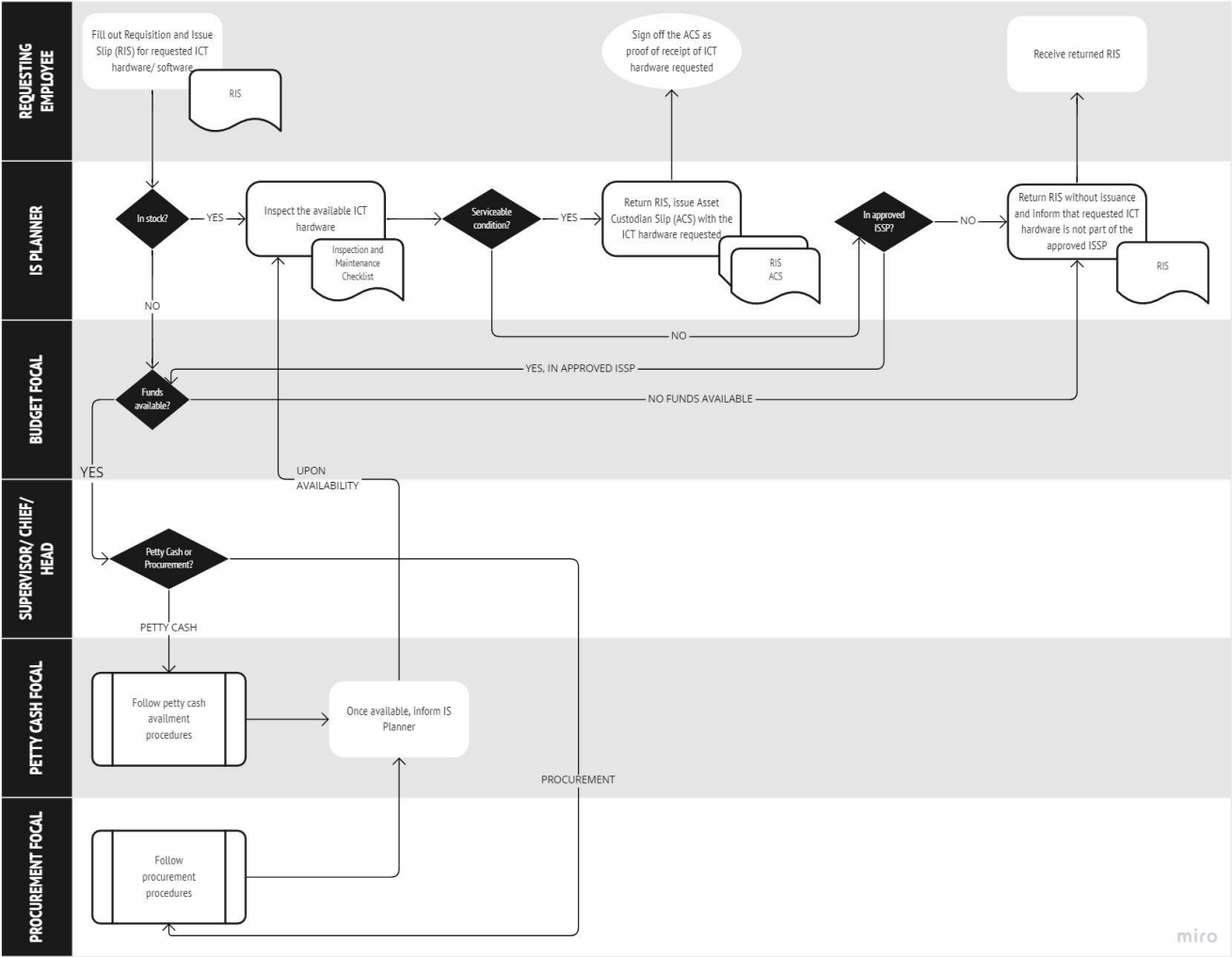
- a. All ICT resources to be acquired shall be reflected in the ISSP.
- b. All costs incurred in the acquisition of ICT resources consisting of the costs of hardware, software components, auxiliary equipment including incidental costs such as delivery, handling, installation, taxes, testing, and IT manpower resources shall be capitalized and charged to the appropriate fixed asset accounts for inventory purposes.
- c. Coordination with the DOTr - Budget Division is necessary to determine the appropriate fixed assets account or other instructions in accordance with the latest rules and regulations from relevant oversight agencies.
- d. All subsequent acquisitions of IT equipment to update/enhance the efficiency or increase the utility of the existing computer system and shall prolong its life shall be charged to the appropriate fixed assets account. Otherwise, said enhancement shall be treated as period cost and recorded in the appropriate expense account.
- e. Preloaded softwares, such as, but not limited to, operating systems that are included in the cost of computer hardware shall be treated as part of the hardware’s cost. Softwares separately purchased shall be recorded as Maintenance and Other Operating Expenses (MOOE) under expense object Supplies and Materials, IT Software or its counterpart pursuant to the latest COA guidelines.
- f. Donated IT resources (e.g., train simulator) shall be recorded in the asset sheet based on fair market value, if the value/amount of the donation is not specified.
- g. Repairs incurred to restore IT assets to good operating condition or to restore and replace broken parts are considered ordinary and recurring expenditures, thus, these are charged to the MOOE.
- h. Major repairs that are needed to correct any extensive deficiency and would lead to the lengthening of the life of the asset shall be accounted for as IT Equipment under Fixed Assets category or its counterpart pursuant to the latest COA guidelines.



VIII. PROCEDURES

A. REQUEST FOR ICT HARDWARE OR SOFTWARE

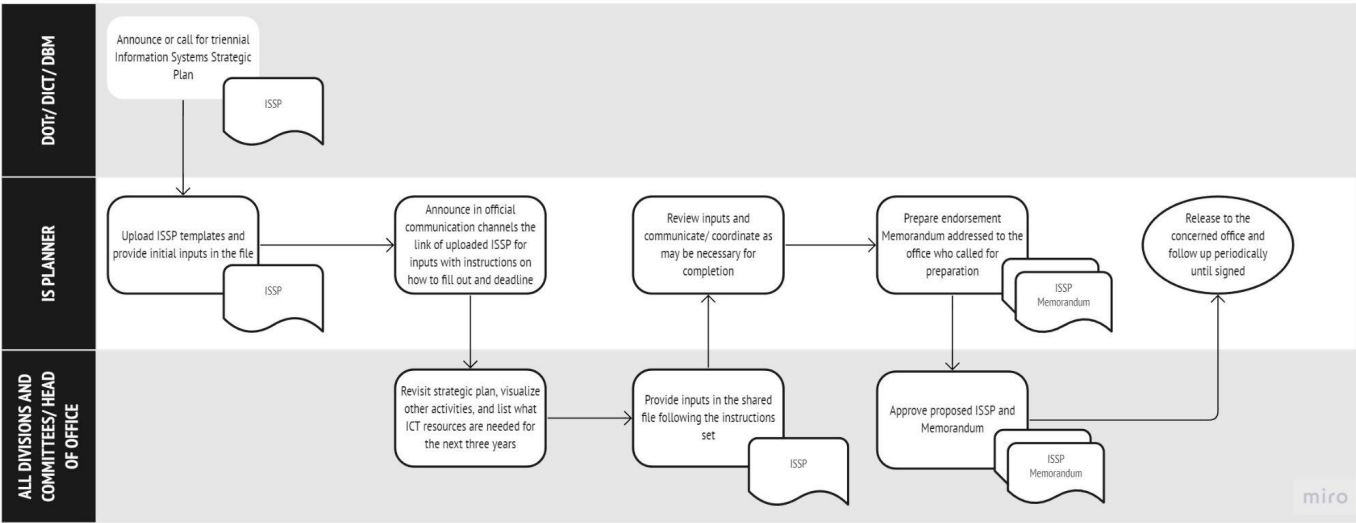
- 1. **Timeline:** Within seven (7) working days if available; if not available, feedback on the next steps containing a working time plan shall be provided to the requesting party within seven (7) working days
- 2. **Type of transaction:** Internal transaction if available; External transaction, if not available [Government to Government (G2G); Government to Business (G2B); or Government to Citizen (G2C)]
- 3. **Forms:**
  - a. Requisition and Issue Slip
  - b. Inspection and Maintenance Checklist






C. PREPARATION OF TRIENNIAL INFORMATION SYSTEMS STRATEGIC PLAN

- 1. **Timeline:** Within one (1) week to three (3) weeks or depending on the deadline set by the DOTr-MIS (excluding approval)
- 2. **Type of transaction:** Internal Transaction; may also be External Transaction - Government-to-Government
- 3. **General Forms involved:**
  - a. ISSP Templates
  - b. Memorandum







	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Acquisition and Issuance of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-AII-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 9 out of 9

**XII. REVIEW AND AMENDMENT**

This Manual shall be amended should there be changes in internal policies or general budgeting and accounting rules. It shall undergo appropriate review, approval, storage, and retention process in accordance with internal procedures on document management.

**PREPARED BY:**

  
**JOSE NOEL G. FLORENDO**  
Engineer II

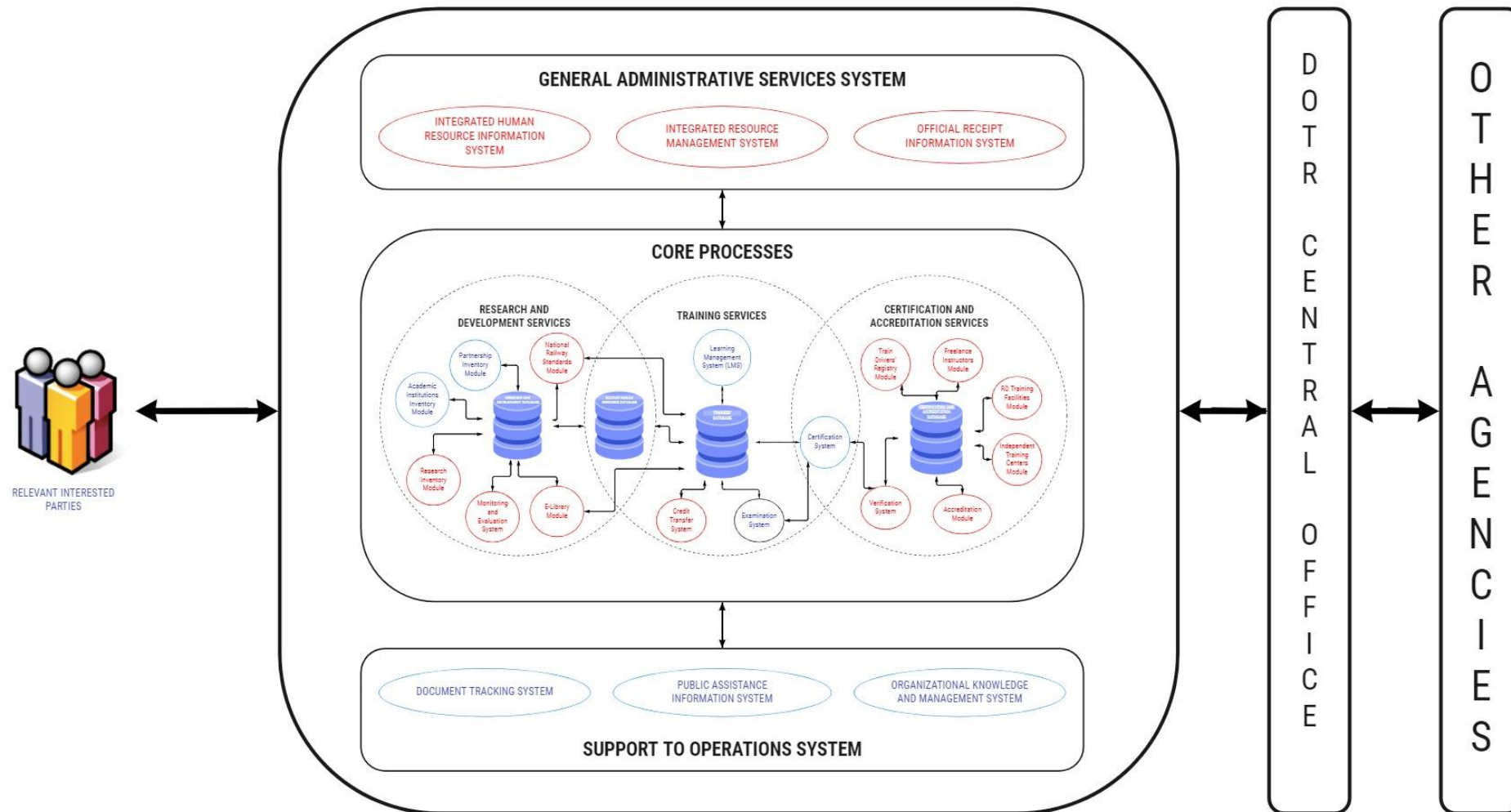
**REVIEWED BY:**


  
**LUISITO G. APACIBLE**  
Head, Technical Committee

**APPROVED BY:**

  
**ANNELI R. LONTOC, CESO I**  
Undersecretary, DOTr  
OIC-ED, PRI

# DOTR-PRI INTEGRATED INFORMATION SYSTEMS



	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Access and Storage of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-ASI-000
		EFFECTIVITY DATE:	SEP 09 2022
		REVISION NO.:	00
		PAGE NO.:	Page 1 out of 8

**MASTER COPY**

Control No.: PRI-ASI-000

Signature: 

## I. OBJECTIVE

The prevalence of technology requires a well-defined access matrix to ensure that data and systems are protected from instances of security breach. Likewise, to ensure efficient resource management, storage and retention policies of relevant data taking up space in storage media of the Philippine Railways Institute (PRI) must be specified.

## II. SCOPE

This Manual shall generally cover the general access and storage policy on the Information and Communication Technology (ICT) resources and its retention period.

Specifically, this Manual shall provide a working procedure for the following:


- Access and Storage Matrix Preparation;
- Access and Storage Matrix Updates for New Provision; and
- Access Termination Procedure.

In view of data pertinent to the electronic documents or records, whether administrative or pertaining to training records, certification records, research records, accreditation records, and other records, the National Archives of the Philippines (NAP) issued its guidelines for all national government agencies and offices to refer to. These are explicitly not included under the scope of this Manual.

## III. DEFINITION OF TERMS

Whenever used in this Manual, the following terms shall have the respective meanings hereinafter set forth:

TERM	DEFINITION
<b>Architecture</b>	: May refer to either hardware or software, or to a combination of both which defines a system's broad outlines and precise mechanisms to function.
<b>ICT Solutions</b>	: The various ICT technologies that are currently existing or will be proposed to run the information systems. Examples of ICT solutions are: for Network - Virtual Private Network, Thin Client; Wireless; for Security - Firewall, Public Key Infrastructure (PKI); for Storage - Storage Attached Network (SAN), Imaging, Warehousing; for Data Capture - Biometrics, Finger Scan, Optical Scan, Optical Mark Reader (OMR), Optical Character Recognition (OCR).

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Access and Storage of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-ASI-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 2 out of 8

TERM	DEFINITION
<b>Information System (IS)</b>	: A system of major processes or operations which facilitates the storage, processing, retrieval and generation of information for decision making, planning, controlling and monitoring purposes. It also refers to a group of related processes (manual or computerized) designed to generate information for the exclusive support of a major functional area of an organization (e.g. Personnel Management Information System, Logistics Management Information System, Financial Management Information System, etc.).
<b>Storage Media</b>	May be offline storage media (i.e. external hard drives, removable magnetic tapes, disks, or optical media, read-only media, flash drives or media, any other physical devices or writing surfaces including, but not limited to tapes, disks, memory chips, printouts onto which information is recorded, stored, or printed within an information system.) or online storage media (i.e. Google Drive, One Drive, Drop box, etc.).

IV. REFERENCE DOCUMENTS

- a. ISO 9001:2015 Standard - Quality Management Systems, specifically 7.5.3 *Control of Documented Information*, which requires organizations to provide clear rules on distribution, access, retrieval, and use of documented information, which in this case is ICT related-documented information except for electronic records.
- b. Republic Act (RA) No. 10173, otherwise known as the “Data Privacy Act of 2012” and its implementing rules and regulations

V. GENERAL ACCESS AND STORAGE POLICY

- a. Each ICT user shall be provided with their respective individual user accounts depending on the ICT system.
- b. Access levels will depend on the system used. In cases of information system applications, supervisors or authorized focal persons may have override access accounts that can access subordinate accounts for business continuity
- c. For a higher level of security and service support, the IS Planner is authorized to have access to Host Administrator/Root Accounts for all IS or ICT Solution, unless otherwise expressly provided.
- d. The standard naming convention used for usernames across all ICT Solution shall be as follows, unless otherwise expressly provided: first letter of the user's first name,




followed by the user's middle initial, and then the user's last name (e.g., If user's full name is Juan G. Dela Cruz, his username shall be *jgdelacruz*).

- e. It is recommended that passwords are a minimum of eight (8) alphanumeric characters and should not consist of common words or variations on the user's name, login name, server name, or PRI name. It is further recommended that users should change their passwords at least every month to ensure optimum security.
- f. It is the responsibility of the user to ensure that his/her password remains a secret, thus, the same shall not be shared with other individuals except when an employee surrenders his/her password as required in this Manual.
- g. Careful use must be exercised with regard to offline electronic storage media as these are inherently unstable since their life expectancy may be affected by various environmental factors such as temperature, electric current fluctuations, humidity, dust, and magnetic fields.
- h. Due diligence must be exercised with regard to online storage media as these are inherently prone to server downtime, accidental deletion, and any other digital vulnerabilities, thus, access levels are important to mitigate risks.
- i. Storage of video and IEC materials beyond the maximum retention period will be considered as unauthorized and may be deleted by the IS Planner upon inspection.

**VI. RETENTION PERIOD**

For the video and IEC materials, the following shall be the retention period per category to save space in the PRI's online and offline storage media:

Video File Category	Minimum Retention Period	Maximum Retention Period
Refresher Training Course Question and Answer Sessions/ Recap Sessions/ Review Sessions	30 days	90 days
Fundamental Training Course	180 days	365 days
Various Stakeholder Online Meetings or Events	30 days	60 days
Audio-Video Presentations or Infomercials	Perpetual unless expressly instructed in a written manner that the same shall be deleted.	

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Access and Storage of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-ASI-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 4 out of 8

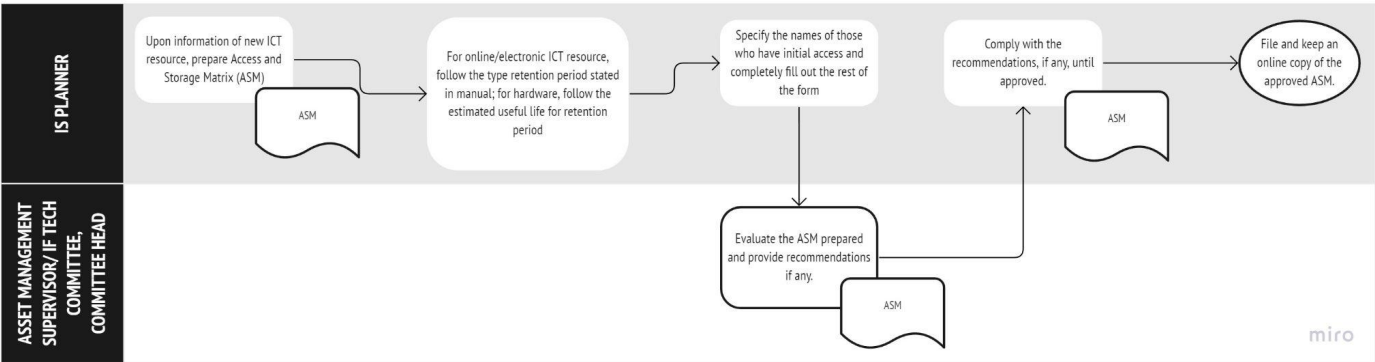
Instructors' Videos	<div>Period of validity of curriculum from which the instructor's video was based</div> <div>Or</div> <div>30 days from the separation from service of the concerned Instructor, provided that the newly-assigned instructor has already recorded the video lecture</div>	<div>180 days from the effectivity of the new curriculum which requires new instructor's video</div> <div>Or</div> <div>90 days from the separation from service of the concerned Instructor or the time whereby the newly-assigned instructor has already recorded the new video lecture, whichever comes first</div>
IEC Materials	Perpetual unless expressly instructed in a written manner that the same shall be deleted.	

For other ICT online resources not explicitly mentioned above, it shall be set on the Access and Storage Matrix to be prepared by the IS Planner. On the other hand, for ICT hardware, the retention period shall follow the estimated useful life of such hardware. It shall be likewise indicated in the Access and Storage Matrix.

VII. PROCEDURE

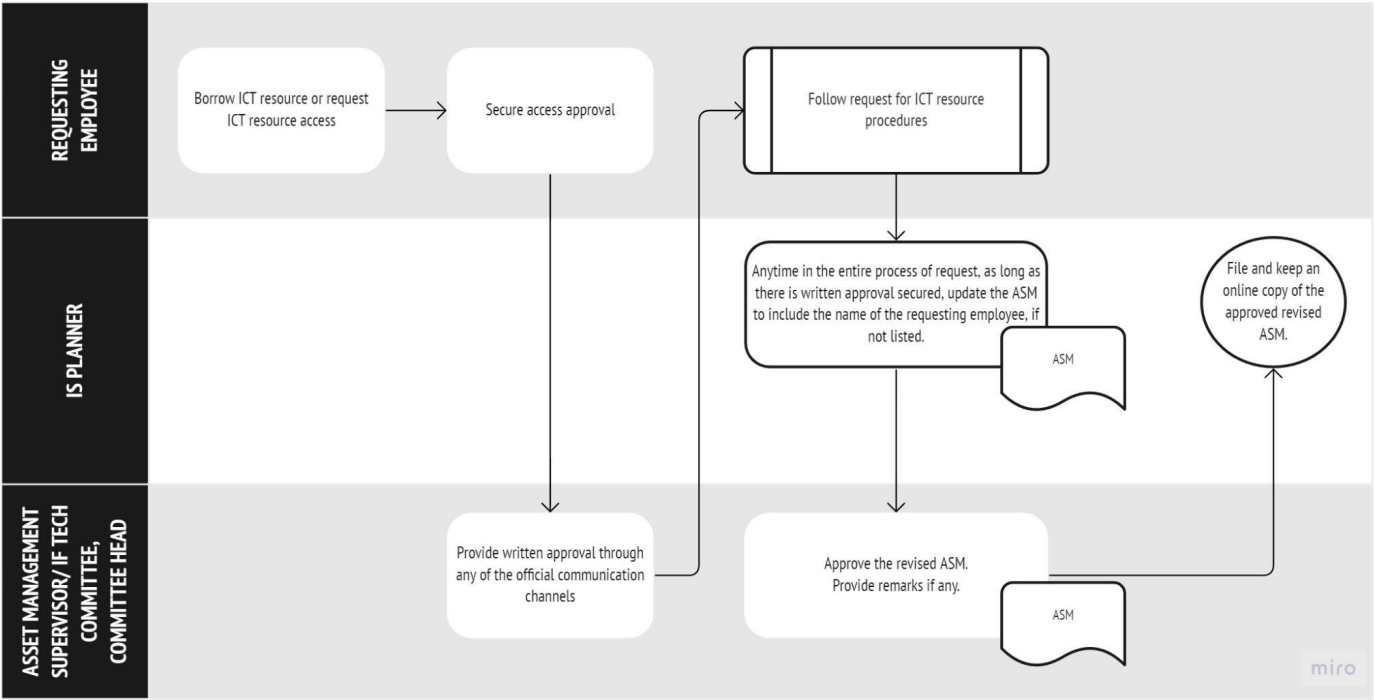
A. ACCESS AND STORAGE MATRIX PREPARATION

- 1. **Timeline:** Within seven (7) working days upon receipt of information of new ICT resource
- 2. **Type of transaction:** Internal transaction
- 3. **Forms:**
  - a. Access and Storage Matrix



**B. ACCESS AND STORAGE MATRIX UPDATES FOR NEW PROVISION**

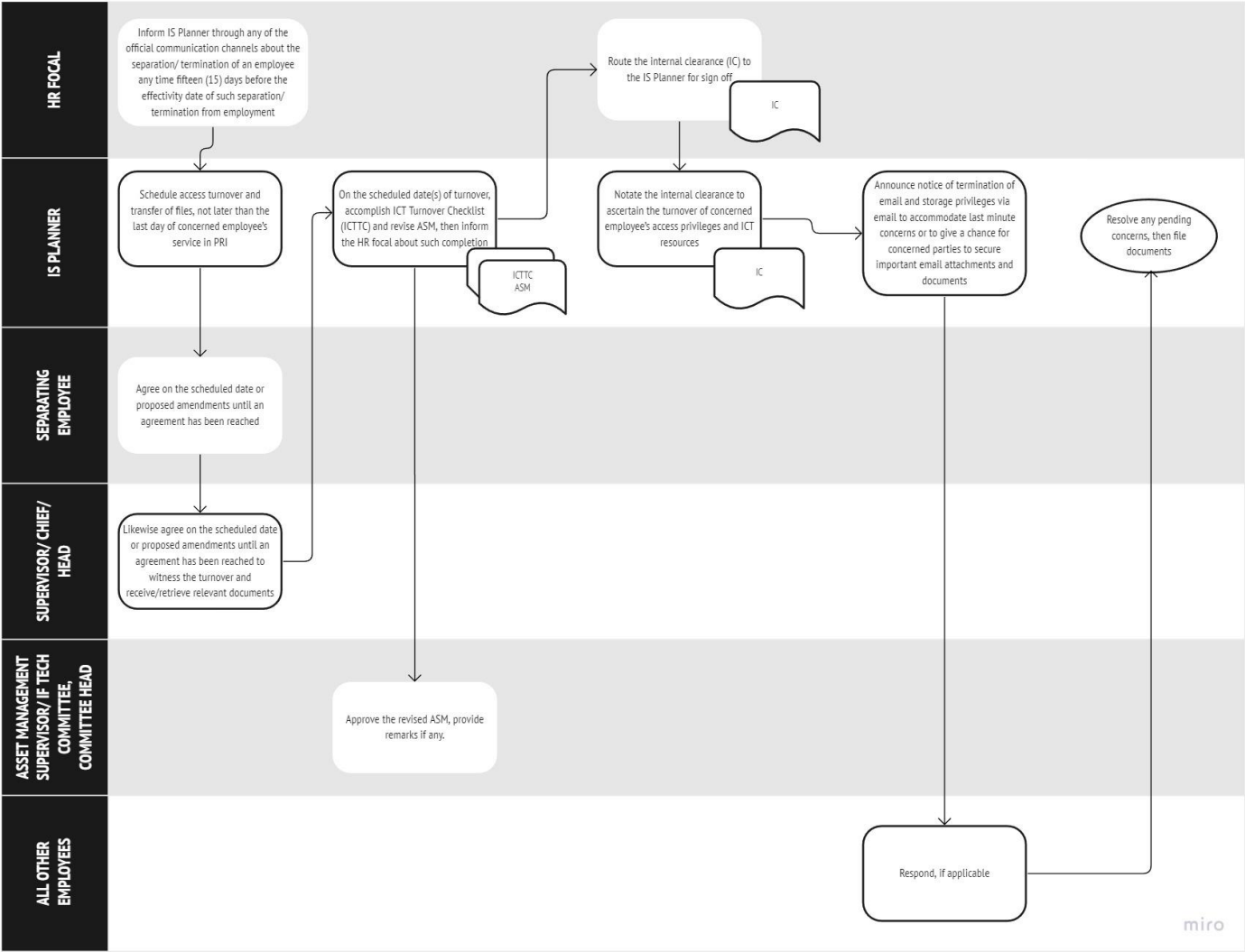
- 1. **Timeline:** Within seven (7) working days from request of new access
- 2. **Type of transaction:** Internal transaction
- 3. **Forms:**
  - a. Access and Storage Matrix






C. ACCESS TERMINATION PROCEDURE

- 1. **Timeline:** Within twenty (20) working days from information about pending resignation/ termination
- 2. **Type of transaction:** Internal transaction
- 3. **Forms:**
  - a. ICT Turnover Checklist
  - b. Access Storage Matrix
  - c. Internal Clearance



	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>Access and Storage of Information and Communication Technology Resources</b>	DOC REF NO.:	PRI-ASI-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 8 out of 8

**VIII. DISSEMINATION**

This Manual shall be cascaded and information, education, and communication materials may be created by the TC as visual aids for its implementation.

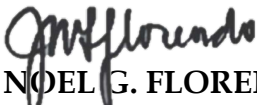
**IX. TRANSITORY PROVISIONS**

The IS Planner and TC shall have thirty (30) working days from the effective date of this Manual to prepare an Access and Storage Matrix for all its existing ICT resources.

**X. REVIEW AND AMENDMENT**

This Manual shall be amended should there be changes in internal policies or general budgeting and accounting rules. It shall undergo appropriate review, approval, storage, and retention process in accordance with internal procedures on document management.

**PREPARED BY:**


  
**JOSE NOEL G. FLORENDO**  
Engineer II


**REVIEWED BY:**

  
**LUISITO G. APACIBLE**  
Head, Technical Committee

**APPROVED BY:**

  
**ANNELI R. LONTOC, CESO I**  
Undersecretary, DOTr  
OIC-ED, PRI

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>General Communications and Email Management</b>	DOC REF NO.:	PRI-GCE-000
		EFFECTIVITY DATE:	SEP 09 2022
		REVISION NO.:	00
		PAGE NO.:	Page 1 out of 10

**DOT - PRI**  
**MASTER COPY**  
 Control No.: PRI-GCE-000  
 Signature: 

## I. OBJECTIVE

Communication methodologies evolved due to the emergence of the fourth industrial revolution. The use of email has been more prevalent due to the changes brought by the new normal and the advancement in technology. Given its regular use in the day-to-day operations of the Philippine Railways Institute (PRI), the following guidelines shall be followed in harmonization with the national laws and policies.

## II. SCOPE


This Manual shall provide for general communication guidelines, email format guidelines, email hazards' description, proper email etiquette, and the procedure for the following:

- a. Request for Email; and
- b. Request for Mailing List/ Distribution List.

## III. DEFINITION OF TERMS

Whenever used in this Manual, the following terms shall have the respective meanings hereinafter set forth:

TERM	DEFINITION
<b>ICT Solutions</b>	: The various ICT technologies that are currently existing or will be proposed to run the information systems. Examples of ICT solutions are: for Network - Virtual Private Network, Thin Client; Wireless; for Security - Firewall, Public Key Infrastructure (PKI); for Storage - Storage Attached Network (SAN), Imaging, Warehousing; for Data Capture - Biometrics, Finger Scan, Optical Scan, Optical Mark Reader (OMR), Optical Character Recognition (OCR).
<b>Information System (IS)</b>	: A system of major processes or operations which facilitates the storage, processing, retrieval and generation of information for decision making, planning, controlling and monitoring purposes. It also refers to a group of related processes (manual or computerized) designed to generate information for the exclusive support of a major functional area of an organization (e.g. Personnel Management Information System, Logistics Management Information System, Financial Management Information System, etc.).

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>General Communications and Email Management</b>	DOC REF NO.:	PRI-GCE-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 2 out of 10


TERM	DEFINITION
<i>Internet</i>	: A worldwide interconnection of millions of computer networks and databases. It is popularly referred to as the Information Superhighway, the Web, or simply as the Net.
<i>Internet Protocol</i>	: A standard set of rules for sending and receiving data through the internet. Each computer or device connected to the internet must have a unique IP address in order to communicate with other systems or the internet
<i>Phishing</i>	: Attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication

IV. REFERENCE DOCUMENTS

- a. DICT Memorandum Circular No. 2015-002, entitled, “Prescribing the Govmail Service Guidelines for Government Agencies”
- b. ISO 9001:2015 Standard - Quality Management Systems, specifically 7.4.(d) - Communication - How to Communicate which requires organizations to determine the method of communication for both internal and external communications

V. GENERAL COMMUNICATION GUIDELINES

- a. For online meetings where external stakeholders are present and there is no provided default virtual background by the meeting/ event organizer, the PRI’s official virtual background shall be used. Such virtual background shall be that announced by the PRI’s Media and Public Affairs Team in any of its managed official channels.
- b. The official communication channel of the Institute shall be Email, Microsoft Teams, Google Chat, or whatever platform that can keep permanent chat records and attachments, as well as maximize productivity.
- c. Use of instant messaging applications like Viber or Whatsapp may be used for instant coordination, however, given the nature of the platform and the risks associated to its usage (i.e., attached files no longer becomes available after a month, chat records may easily be erased since membership is by mobile number instead of email address, etc.), the same is not encouraged for prolonged usage and planning.

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>General Communications and Email Management</b>	DOC REF NO.:	PRI-GCE-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 3 out of 10

d. For Email:

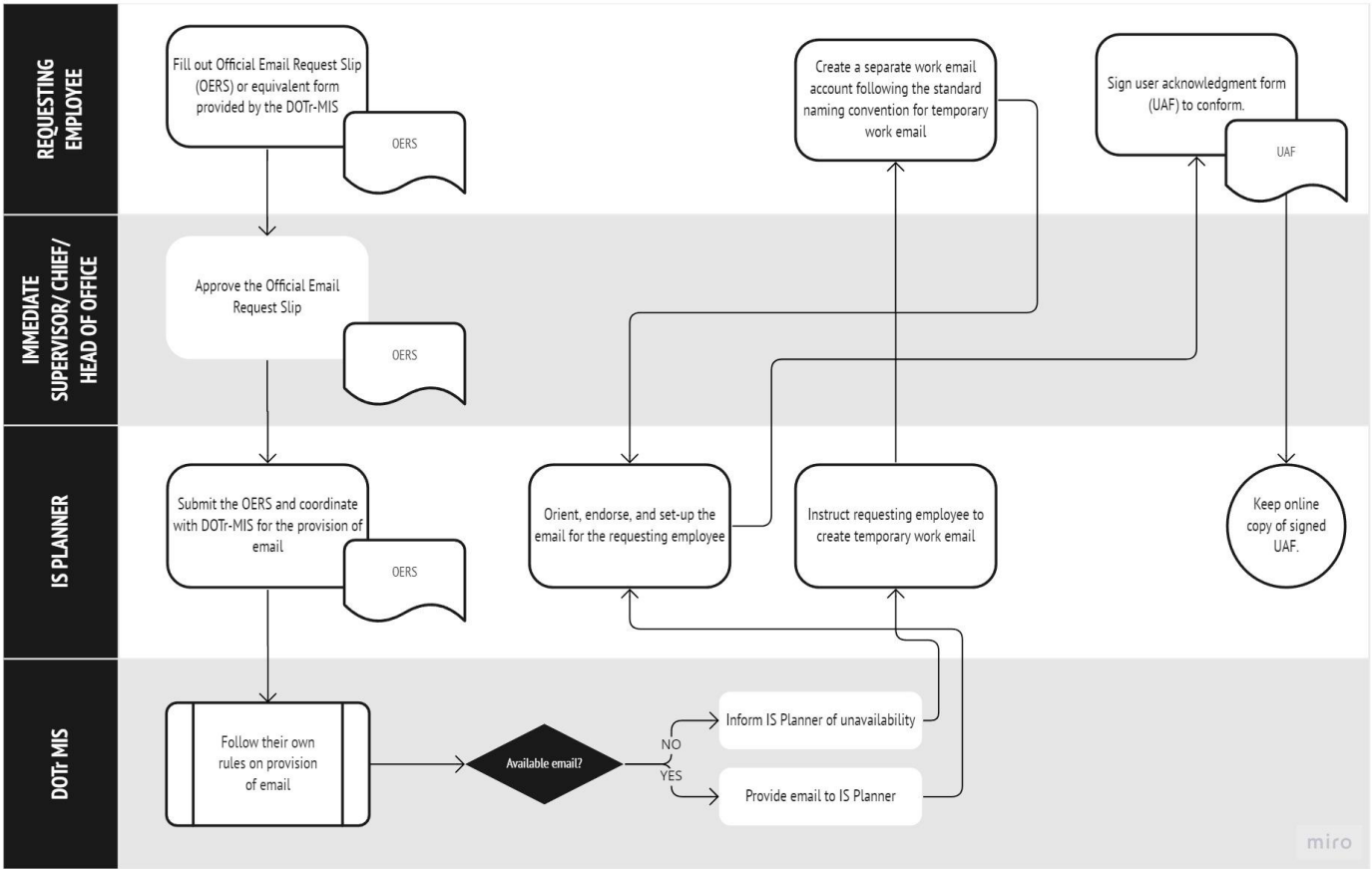
1. Employee Email Account: Users shall be responsible for its maintenance and security.
2. Division or Non-Personnel Accounts shall be provided to divisions and sections, and shall be used as the means for communication between the government and the general public as a channel for first contact, unless the DOTr-MIS responds that there is no available email slot to be provided.
3. The division or other non-personnel accounts shall be published in the PRI’s website as part of its compliance with Republic Act 9485, otherwise known as the Anti-Red Tape Act of 2007.
4. The administrator of the PRI’s email account shall be the IS Planner.
5. For the non-employee/ division or section accounts, the administrator shall be the respective divisions’ document controllers.
6. For the PRI’s email account, the IS Planner shall exercise sound discretion on the organization and management of emails, including the forwarding of the same to the appropriate divisions or sections’ email addresses, provided that for emails requesting for action from any of the PRI personnel, the same must be forwarded to the ED for further instructions, copy furnish (cc) the concerned division/section.



VI. PROCEDURE

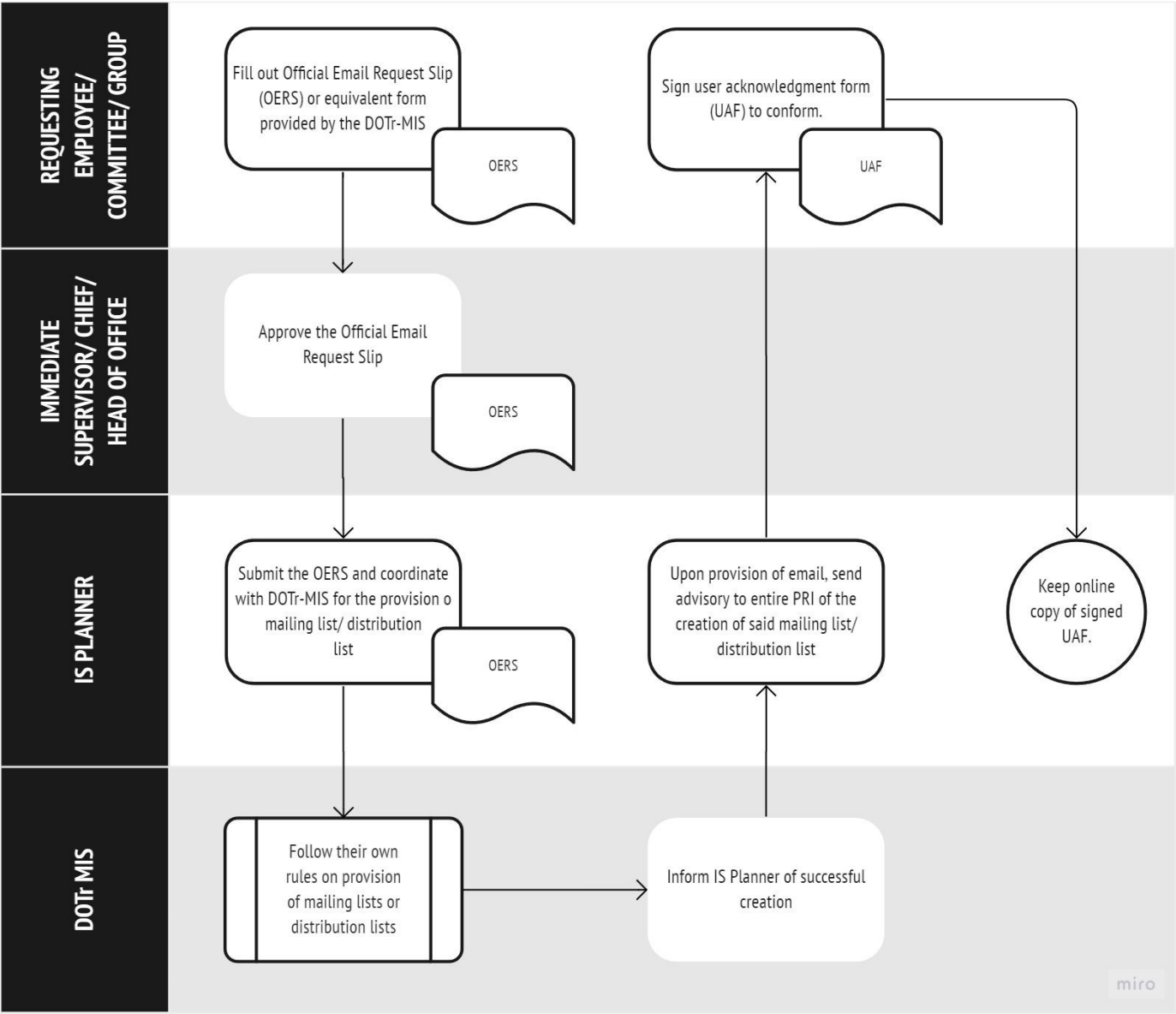
A. REQUEST FOR EMAIL

- 1. **Timeline:** Within seven (7) working days
- 2. **Type of transaction:** Internal transaction
- 3. **General Forms involved:**
  - a. Official Email Request Slip
  - b. User Acknowledgement Form



**B. REQUEST FOR MAILING LIST/ DISTRIBUTION LIST**

- 1. **Timeline:** Within seven (7) working days from request
- 2. **Type of transaction:** Internal transaction
- 3. **General Forms involved:**
  - a. Official Email Request Slip
  - b. User Acknowledgement Form



	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>General Communications and Email Management</b>	DOC REF NO.:	PRI-GCE-000
		EFFECTIVITY DATE:	SEPT 09,2022
		REVISION NO.:	00
		PAGE NO.:	Page 6 out of 10

**VII. EMAIL GUIDELINES ON EMAIL FORMAT**

**A. Official Email Template**

Pursuant to the DICT guidelines mentioned above, all personnel are recommended to follow the email templates for the Formal Email, Quick Email, Person-to-Person, and Quick Response.

**B. Official Email Template**

Pursuant to the Circular mentioned above, all personnel shall follow the email template as follows:

1. Annex C - Formal Letter;
2. Annex D - Office Memorandum;
3. Annex E - Person-to-Person; and
4. Annex F - Quick Response.

**C. Official Email Signature**


1. All official email accounts shall be provided with an official signature that shall be used to achieve an enterprise identity for the Institute and provide a standardized look in the perspective of external stakeholders. Pursuant to the aforementioned Circular, the following shall be the standard content of the official email signature:

Complete Employee Name  
Position / Designation  
Unit / Section / Division / Office  
Complete Agency Address  
Telephone / Fax Number  
URL

Example:

Juan B. Dela Cruz  
Planning Officer II  
Internal Planning and Monitoring Office  
DOST-Agency  
ICTO Building  
C.P. Garcia Avenue  
U.P. Campus, Diliman



	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>General Communications and Email Management</b>	DOC REF NO.:	PRI-GCE-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 7 out of 10

1101 Quezon City  
PHILIPPINES  
Tel. (+63-2)920-0101  
[www.icto.dost.gov.ph](http://www.icto.dost.gov.ph)

2. As a form of public information dissemination, event promotion or notification may be included, just below the email signature, as illustrated below:

Example:

**PCSC 2009**  
[<http://ccs.su.edu.ph/pcsc2009>]  
9th Philippine Computing Science Congress  
March 2-3, 2009  
Silliman University  
Dumaguete City, PHILIPPINES

Organized by:  
COMPUTING SOCIETY OF THE PHILIPPINES (CSP)  
[www.csp.org.ph](http://www.csp.org.ph)


**FINAL CALL FOR PAPERS / PARTICIPATION**

*The Computing Society of the Philippines (CSP) invites you to participate and submit papers in the 9th Philippine Computing Science Congress (PCSC 2009). The CSP organizes this conference to enable local and neighboring computing educators, researchers, and JCT professionals and students to interact and to share their work in computing, computer science, computer engineering, computational science, and information and communications technology (ICT).*

*The conference features special lectures by prominent researchers and educators in the field of information and communications technology (including computing, computer science, computer engineering, computational science, and related disciplines). It also features contributed research papers on computing and ICT.*

3. All email shall use a standard disclaimer, such as:

*The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed and other parties authorized to receive it. It may contain confidential or legally privileged communication. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this*

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>General Communications and Email Management</b>	DOC REF NO.:	PRI-GCE-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 8 out of 10

*information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this e-mail and then immediately delete it from your system. Opinions contained in this e-mail or any of its attachments do not necessarily reflect the opinions of the PRI or the Department of Transportation.*

**VIII. DESCRIPTION OF EMAIL HAZARDS**


Any user shall not use the email for purposes that are illegal, inappropriate, or disallowed by the Institute, such as the following:

- a. Chain Mail: Personal email that attempts to induce the recipient to make a number of copies of the letter and then pass them on to as many recipients as possible;
- b. Harassing or hate mail: Any threatening or abusive email sent to individuals or organizations which violates the Institute’s or DOTr’s policies or rules;
- c. Sending Viruses: Any malicious computer codes that include, but are not limited to, computer virus, Trojan horse, worm, and hoax;
- d. Spam or email bombing attacks: Any intentional email transmissions that disrupt normal email service;
- e. Junk mail: Any unsolicited email that is not related to the Institute’s or DOTr’s business and is sent without a reasonable expectation that the recipient would be welcome receiving it; and
- f. Using false identification: Actions that defraud another or misrepresent or fail to accurately identify the sender; It is the responsibility of the user to maintain his/her emails (i.e., to delete unwanted files and to save those that are required for archiving).

**IX. PROPER EMAIL ETIQUETTE**

The following is a comprehensive list of proper email etiquette:


- a. Be sure to include a descriptive subject line.
- b. Consider using a mailing list or BCC to keep email addresses private or to ensure that the "To:" area of the message remains a small size.

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>General Communications and Email Management</b>	DOC REF NO.:	PRI-GCE-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 9 out of 10

- c. Write clear, concise, and specific messages. Clearly state terms and conditions to avoid miscommunication, especially when providing information about times, places, or people.
- d. Avoid double spacing your messages as email requires recipients to scroll through messages without the benefit of highlighting or marking the message as one might on a printout.
- e. Avoid the use of all capital letters and colored fonts.
- f. When replying to a message, consider deleting part/s of the original message to save space on the screen. Retain only the part/s of the sender's message to which you are responding.
- g. Avoid using the “Reply To All” function as this allows sending your response to all recipients of the e-mail.
- h. Avoid acronyms because not everyone will know their respective meanings.
- i. Use proper grammar and conduct a spell check of your messages.
- j. Use simple fonts because computers may have a limited number of fonts available for email use. Using a small or compact font keeps the message in a more confined area.
- k. Leave the address field blank and fill it out last, to avoid sending unchecked or hastily written messages.
- l. Do not use unnecessary punctuations, text messaging shortcuts, and slang language.
- m. Avoid emoticons.
- n. Remain gender neutral.
- o. Keep harassment and discrimination policies in mind.
- p. Never reply to spam messages.
- q. Ask permission before forwarding messages.
- r. Be cautious when sending attachments, especially those that are considered confidential.
- s. Always use salutations and signatures.

**X. DISSEMINATION**


This Manual shall be cascaded and information, education, and communication materials like flowcharts may be created by the TC as visual aids for its implementation.

	<b>PHILIPPINE RAILWAY INSTITUTE</b> Quality Management System  <b>General Communications and Email Management</b>	DOC REF NO.:	PRI-GCE-000
		EFFECTIVITY DATE:	SEPT 09, 2022
		REVISION NO.:	00
		PAGE NO.:	Page 10 out of 10

**XI. REVIEW AND AMENDMENT**

This Manual shall be amended should there be changes in email management. It shall undergo appropriate review, approval, storage, and retention process in accordance with internal procedures on document management.

**PREPARED BY:**

  
**JOSE NOEL G. FLORENDO**  
Engineer II

**REVIEWED BY:**

  
**LUISITO G. APACIBLE**  
Head, Technical Committee

**APPROVED BY:**

  
**ANNELI R. LONTOC, CESO I**  
Undersecretary, DOTr <sup>PMB</sup>  
OIC-ED, PRI



Republic of the Philippines  
**DEPARTMENT OF TRANSPORTATION**

**USER ACKNOWLEDGMENT FORM**

As in any written policy, the challenge of effectively and efficiently implementing a policy is in the education of all affected parties. Thus, this document is meant to be signed by the authorized user only after he or she has received the appropriate orientation or education about this document from the

I have read and understood the Agency's e-mail service policy and agree to abide by it.

I understand that any violation of the above policies and procedures may result in disciplinary action, up to and including termination from government service or termination of contract.

Complete Name :  
Designation :  
Office / Unit :  
Official Email Address :  
Telephone Number :

---

Signature

---

Date Signed

*For any questions or clarifications about this policy, address them to the Head of the \_\_\_\_\_ or Agency's Email Account Administrator before signing. If you do not have any question, the Agency presumes that you have fully understood this e-mail policy and shall adhere to it at all times.*