

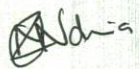


KENYA PLANT HEALTH INSPECTORATE SERVICE

Business Continuity Plan for ICT Department

BCM/KEPHIS/ICT/001

DOCUMENT CONTROL

	NAME AND TITLE	SIGNATURE	DATE
Author	Deputy Director ICT & Innovation		04/12/24
Approved	Director Corporate Services		06/12/2024
Release Authority	Managing Director		9/12/2024
Maintenance	ICT Department		
Distribution	This document will be maintained by the Department for controlled access. Copies can be availed for download via staff email.		

REVISION DETAILS

REVISION NUMBER	REVISION SUMMARY	REVISED BY	SIGNATURE	DATE

Contents

Background.....	4
PURPOSE.....	5
SCOPE	5
JUSTIFICATION	6
METHODOLOGY.....	7
Export process - Request for inspection.....	7
Export process - Assign, pass/reject issue certificates.....	10
Import Process – PIP Processing	13
Seed Certification and Plant Variety Protection Process	15
ERP System and Email system processes	17
RISK MAPPING	19

Background

Kenya Plant Health Inspectorate Service (KEPHIS) is a regulatory body that was established under the State Corporations Act (CAP 446) pursuant to Legal Notice No. 305 of 18th October 1996. KEPHIS operates under the KEPHIS Act No.54 of 2012. KEPHIS is mandated to implement the Agriculture Produce (Export) Act (CAP 319), Plant Protection Act (CAP 324), and the Seeds and Plant Varieties Act (CAP 326). The role of the Corporation is to undertake regulatory function in the agricultural sector in matters relating to plant protection, seeds and plant varieties that assures the quality of agricultural inputs and produce, thereby promoting sustainable agricultural and economic growth. The functions of KEPHIS as encapsulated in the KEPHIS Act No. 54 of 2012 are to:

- (a). Regulate matters relating to plant protection, seeds and plant varieties;
- (b). Administer and enforce Sanitary and Phytosanitary measures;
- (c). Support the administration and enforcement of food safety measures;
- (d). Establish service laboratories to monitor the quality and levels of toxic residues in agro-inputs, irrigation water, plants, soils and produce;
- (e). Be the principal advisor to the Government on issues relating to seeds and planting material;
- (f). Implement plant variety protection in Kenya, administer plant breeders' rights and maintain the Plant Breeders' Rights Register;
- (g). Undertake plant variety testing and description, seed certification and plant quarantine control;
- (h). Undertake inspection and grading of plants and plant produce at the ports of entry and exit;
- (i). In consultation with other relevant agencies, develop and implement standards for seed and plant materials;
- (j). Implement and enforce national biosafety regulations on the introduction and use of genetically or living modified species of plants, insects and micro-organisms, plant products and other related species;
- (k). Regulate import and export of plants and plant materials;

(l). In consultation with other relevant agencies, regulate the commercial exploitation of naturally occurring plants and plant-related microorganisms;

(m). Register and license seed merchants, seed growers, agents and any other person who may be required to be registered under the provisions of this Act or any of the laws specified in the First Schedule;

(n). Enter into association with such other bodies or organizations or authorized persons as the Board may consider desirable or appropriate in furtherance of the purposes for which the Service is established;

(o). Be the liaison office for international conventions relating to plant variety protection, plant protection, seed certification and dealing with endangered species or any other related conventions.

KEPHIS as a science-based organization relies heavily on technology in its functions for delivery on the institutional mandate. There are technological advancements in many areas touching on the core mandate which include; automated issuing of phytosanitary certificates and ephytos for exports, which are then transmitted to the receiving party via a secure transportation protocol through integration with IPPC ePhyto hub, issuance of plant import permits, inspection certificates and cargo release through the IEICS system, seed certification and plant variety protection through the SCPVP system aimed at reducing time and transaction costs by providing an online payment option for the seed industry and plant breeders, automation of Finance, Human Capital, Supply Chain Management, fleet management, accommodation and meeting rooms booking through the ERP system and email system for communication.

PURPOSE

The purpose of this document is to develop a framework for the management of risks and disasters to ensure ICT business continuity and at Kenya Plant Health Inspectorate Service (KEPHIS). This will help ICT department in handling ICT disruptions to its Infrastructure (Network, servers, mobile devices) and Services (Automated processes, partners and suppliers) within the prescribed time frames. KEPHIS as an institution emphasizes a proactive approach to risk management rather than reacting to disasters.

SCOPE

This plan will only address the recovery of systems under the direct control of ICT Department and that are critical for business continuity.

These critical activities include the following:

- Administration of IT assets and resources

- Software systems management
- Network Infrastructure and Management
- Performing backup and recovery
- Provision of user support
- Managing relationships with service providers

OBJECTIVE

- a) The document seeks to fulfill the following objectives in the context of KEPHIS operations
- a) Maximize the effectiveness of Business Continuity operations through established procedures that consist of the following phases:
- Notification/Damage Assessment Phase
 - Activation Phase
 - Mobilization Phase
 - Recovery Phase
 - Return to Normal Phase
- b) Establish comprehensive awareness and training to ensure IT staff are familiar with the plan;
- c) Preventing the loss of the Services' resources such as hardware, data and physical ICT assets;
- d) Minimizing downtime related to ICT
- e) Keeping the business running in the event of a disruption
- f) Define the inherent risks in the operations.
- g) Develop mitigation strategies for the identified risks.
- h) Define what a disaster is and the procedure of declaring it.

JUSTIFICATION

The risks inherent in the operations at KEPHIS and their potential impact on business in the industry necessitate the need for a ICT business continuity management framework for the following reasons:

- The industry serviced by the KEPHIS operations is very sensitive to business disruptions.
- The products involved are highly perishable and cannot tolerate long periods of business delays.

- The potential loss of revenue to the country and the institution due to business disruption is enormous.
- The institutional credibility is adversely affected by operational disruptions both locally and internationally.

METHODOLOGY

This framework includes ICT Business Continuity Management plan with activities showing the Risk Profile and Risk maps outlined as below;

- Identification of critical KEPHIS processes to help in the identification and assessment of the risk prone areas.
- Identification and assessment of the various risks inherent in each process.
- Definition of mitigation strategies, tolerance levels and responsibilities for each risk identified.
- Mapping out of the various risks based on probability of occurrence and potential impact.
- Definition of communication and response procedures in the event of risk occurrence for each of the risks identified.

For each risk identified a number of attributes were defined as shown in the following tables. These include: Probability (how likely to happen), Impact, Functions/process affected, Probable cause, Proximity (when likely to happen), Mitigation, Mitigation Responsibility, Early warning Indicators, Tolerance levels, constraints, Resources, disaster response and responsibilities

Export process - Request for inspection

Possible risk	Clients' inability to make and submit an application for inspection of consignments
Probability (How likely to happen)	Seldom
Impact	Critical
Functions /process affected	Export and import certification processes

Probable cause	Internet unavailability, IEICS system unavailable, LAN/WAN failure, major system changes/upgrade, system under capacity, IEICS server failure, Malware attacks
Proximity (when likely to happen)	Any time throughout the year
Mitigation Strategies	- Move critical systems to the cloud(IEICS, SCPVP) - Maintain redundant internet link - Maintain redundant system setup for IEICS. - Maintain redundant core LAN/WAN equipment - Engage a reliable Internet Service Provider (ISP.) - Regularly train and create awareness whenever there are major system changes or upgrades. - Install antimalware tools and regular staff sensitization on cyber security. - Establish a help desk to manage customer relationships.
Mitigation Responsibility	Deputy Director ICT & Innovation
Early warning Indicators	- Frequent system breakdowns - Frequent user/customer complaints - Degradation in system performance levels
Tolerance levels	5 hours
Constraints	- Inadequate financial and human resources. - External players: (ISPs, Kenya Power)
Resources	- Preventive Maintenance costs. - Redundant link costs.

	- Redundant system setup for IEICS costs. - Redundant core LAN/WAN systems costs. - Antimalware tools and staff sensitization on information security - Mailing system cost - Training and Awareness costs. - Helpdesk system and personnel.
Action/response	- Once the client/user notices that the risk has materialized he/she communicates to the help desk. - The help desk informs ICT department, the Principal ICT officers who should then establish the cause and the approximate time of restoration by the relevant ICT officers. - If resolution is likely to take more than one hour or has persisted for more than 30 minutes, the Principal ICT officers should inform the Deputy Director ICT & Innovation. - If problem persists for more than two hours, Deputy Director ICT & Innovation informs the Director Corporate Services and keeps updating regularly on the progress. - If problem persists for more than three hours, Director Corporate Services informs the Managing Director and keeps updating regularly on the progress - If the problem persists for more than five hours, the Managing Director declares the issue a disaster and invokes the disaster operational process as follows ; - o Director Phytosanitary & Biosecurity communicates to the clients on the system status through mail and notices and send a fillable Phytosanitary certificate form to the clients to fill in and print on a regular paper and present to KEPHIS officer after inspection. - o Clients to proceed with the inspection process by presenting the original copies of consignment documents. - o If inspection is successful the KEPHIS officer uses the filled Phytosanitary certificate form filled by the client to produce

	a phytosanitary certificate through photocopying on security paper and stamps in the certificate number (emergency security papers should be pre-coded for ease of traceability) ○ KEPHIS officer ensures the client records the serial number of the phytosanitary certificate, the name of the company and who collected the certificate in the black book.
Responsibility	Director Phytosanitary & Biosecurity, Deputy Director ICT & Innovation

Export process - Assign, pass/reject issue certificates

Possible risk	Users unable to allocate, pass/reject consignments and issue Phytosanitary certificates
Probability (how likely to happen)	Seldom
Impact	Critical
Functions /process affected	Export and import certification processes
Probable cause	IEICS system failure, LAN/WAN failure at KEPHIS offices, major system changes/upgrade, system under capacity, mail server failure, IEICS server failure, Malware attacks
Proximity (when likely to happen)	Any time throughout the year
Mitigation Strategies	- Move critical systems to the cloud (IEICS, SCPVP) - Maintain redundant internet link. - Maintain redundant system setup for IEICS. - Maintain redundant core LAN/WAN

	- Engage a reliable Internet Service Provider (ISP). - Install antimalware tools and regular staff sensitization on cyber and information security. - Regularly train and create awareness whenever there are major system changes or upgrades. - Establish a help desk to manage customer relationships.
Mitigation Responsibility	Deputy Director ICT & Innovation
Early warning Indicators	- Frequent system breakdowns. - Frequent user/customer complaints. - Degradation in system performance levels.
Tolerance levels	5 hours
Constraints	- Inadequate financial and human resources. - External players: (ISPs, Kenya Power)
Resources	- Preventive Maintenance costs. - Redundant link costs. - Redundant system setup for IEICS costs. - Redundant core LAN/WAN systems costs. - Training and Awareness costs. - Antimalware tools and staff sensitization on information security - Mailing system cost - Helpdesk system and personnel.
Action/response	- Once the client/user notices that the risk has materialized he/she communicates to the help desk.

	- The help desk informs ICT department, the Principal ICT officers who should then establish the cause and the approximate time of restoration by the relevant ICT officers. - If resolution is likely to take more than one hour or has persisted for more than 30 minutes, the Principal ICT officers should inform the Deputy Director ICT & Innovation. - If problem persists for more than two hours, Deputy Director ICT & Innovation informs the Director Corporate Services and keeps updating regularly on the progress. - If problem persists for more than three hours, Director Corporate Services informs the Managing Director and keeps updating regularly on the progress - If the problem persists for more than five hours, the Managing Director declares the issue a disaster and invokes the disaster operational process as follows ; - o Director Phytosanitary & Biosecurity communicates to the clients on the system status through mail and notices and send a fillable Phytosanitary certificate form to the clients to fill in and print on a regular paper and present to KEPHIS officer after inspection. - o Clients to proceed with the inspection process by presenting the original copies of consignment documents. - o If inspection is successful the KEPHIS officer uses the filled Phytosanitary certificate form filled by the client to produce a phytosanitary certificate through photocopying on security paper and stamps in the certificate number (emergency security papers should be pre-coded for ease of traceability) - o KEPHIS officer ensures the client records the serial number of the phytosanitary certificate, the name of the company and who collected the certificate in the black book.
Action Responsibility	Director Phytosanitary & Biosecurity, Deputy Director ICT & Innovation

Import Process – PIP Processing

Possible risk	Personnel unable to process Plant Import Permit (PIP)
Probability (how likely to happen)	Seldom
Impact	Critical
Functions /process affected	Import certification processes
Probable cause	IEICS System failure Hardware failure Malware attacks
Proximity (when likely to happen)	Any time throughout the year
Mitigation Strategies	- Move critical systems to the cloud (IEICS, SCPVP) - Maintain redundant internet link. - Maintain redundant system setup for IEICS. - Maintain redundant core LAN/WAN - Engage a reliable Internet Service Provider (ISP). - Regularly train and create awareness whenever there are major system changes or upgrades. - Install antimalware tools and regular staff sensitization on cyber and information security. - Establish a help desk to manage customer relationships.

Mitigation Responsibility	Deputy Director ICT & Innovation
Early warning Indicators	- Frequent IEICS system breakdowns. - Frequent user/customer complaints. - Increased political uncertainties.
Tolerance levels	Six hours
Constraints	- Inadequate financial and human resources. - External players: (ISPs, Kenya Power)
Resources	- Redundant core LAN/WAN systems costs. - Training sensitization and Awareness costs. - Antimalware tool costs - Helpdesk system and personnel.
Action/response	- Once a user notices that the risk has materialized he/she communicates to the help desk. - The help desk informs ICT department, the Principal ICT officers who should then establish the cause and the approximate time of restoration by the relevant ICT officers. - If resolution is likely to take more than one hour or has persisted for more than 30 minutes, the Principal ICT officers should inform the Deputy Director ICT & Innovation. - If problem persists for more than two hours, Deputy Director ICT & Innovation informs the Director Corporate Services and keeps updating regularly on the progress. - If problem persists for more than three hours, Director Corporate Services informs the Managing Director and keeps updating regularly on the progress - If the problem persists for more than six hours, the Managing Director declares the issue a disaster and invokes the disaster operational process as follows;

	○ Director Phytosanitary & Biosecurity communicates to the clients on the system status through mail and notices and authorizes manual processing of PIPs.
Action Responsibility	Director Phytosanitary & Biosecurity, Deputy Director ICT & Innovation

Seed Certification and Plant Variety Protection Process

Possible risk	Staff and client inability to access the SC&PVP system
Probability (how likely to happen)	Seldom
Impact	Moderate
Functions /process affected	Seed Certification and Plant Variety Protection process
Probable cause	- SC&PVP system failure, LAN/WAN failure at KEPHIS offices, major system changes/upgrade, system under capacity, mail server failure, SC&PVP server failure, Malware attacks
Proximity (when likely to happen)	Any time throughout the year.
Mitigation	- Move critical systems to the cloud (IEICS, SCPVP) - Maintain redundant internet link. - Maintain redundant system setup for SC&PVP - Maintain redundant core LAN/WAN - Engage a reliable Internet Service Provider (ISP).

	- Install antimalware tools and regular staff sensitization on cyber and information security. - Regularly train and create awareness whenever there are major system changes or upgrades. - Establish a help desk to manage customer relationships.
Mitigation Responsibility	Deputy Director ICT & Innovation
Early warning Indicators	- Frequent SC&PVP system breakdowns. - Frequent user/customer complaints.
Tolerance levels	1 day
Constraints	- Inadequate financial and human resources. - External players (KRA, Kenya Police Service, KAA)
Resources	- Redundant core LAN/WAN systems costs. - Antimalware tools and staff sensitization on information security - Mailing system cost - Training and Awareness costs. - Helpdesk system and personnel.
Action/response	- Once the client/user notices that the risk has materialized he/she communicates to the help desk. - The help desk informs ICT department, the Principal ICT officers who should then establish the cause and the approximate time of restoration by the relevant ICT officers. - If resolution is likely to take more than one hour or has persisted for more than 1 hour, the Principal ICT officers should inform the Deputy Director ICT & Innovation. - If problem persists for more than three hours, Deputy Director ICT & Innovation informs the Director Corporate Services, Director Seed

	Certification & Plant Variety Protection and keeps updating regularly on the progress. - If problem persists for more than six hours, Director Corporate Services informs the Managing Director and keeps updating regularly on the progress - If the problem persists for more than one day, the Managing Director declares the issue a disaster and invokes the disaster operational process as follows; - o Director Seed Certification & Plant Variety Protection communicates to the clients on the system status through mail and notices and authorizes manual processing.
Action Responsibility	Director Seed Certification & Plant Variety Protection, Deputy Director ICT & Innovation

ERP System and Email system processes

Possible risk	Staff and client inability to access the ERP system its associated portals or Email System
Probability (how likely to happen)	Seldom
Impact	Minor
Functions /process affected	ERP system processes Email system access
Probable cause	- ERP system failure, Email system failure, LAN/WAN failure at KEPHIS offices, major system changes/upgrade, system under capacity, mail server failure, Malware attacks
Proximity (when likely to happen)	Any time throughout the year.

Mitigation	- Regular preventive maintenance of ERP and Email servers - Maintain redundant internet link. - Maintain UpToDate backup copies - Maintain redundant core LAN/WAN - Engage a reliable Internet Service Provider (ISP). - Install antimalware tools and regular staff sensitization on cyber and information security. - Regularly train and create awareness whenever there are major system changes or upgrades. - Establish a help desk to manage customer relationships.
Mitigation Responsibility	Deputy Director ICT & Innovation
Early warning Indicators	- Frequent ERP or Email system breakdowns. - Frequent user/customer complaints.
Tolerance levels	2 days
Constraints	- Inadequate financial and human resources. - External players (KRA, Kenya Police Service, KAA)
Resources	- Redundant core LAN/WAN systems costs. - Antimalware tools and staff sensitization on information security - ERP system cost - Mailing system cost - Training and Awareness costs. - Helpdesk system and personnel.
Action/response	- Once the user notices that the risk has materialized he/she communicates to the help desk. - The help desk informs ICT department, the Principal ICT officers who should then establish the cause and the approximate time of restoration by the relevant ICT officers.

	- If resolution is likely to take more than two hour or has persisted for more than 1 hour, the Principal ICT officers should inform the Deputy Director ICT & Innovation. - If problem persists for more than three hours, Deputy Director ICT & Innovation informs the Director Corporate Services and keeps updating regularly on the progress. - If problem persists for more than six hours, Director Corporate Services informs the Managing Director and keeps updating regularly on the progress - If the problem persists for more than two days, the Managing Director declares the issue a disaster and invokes the disaster operational process as follows; - o Director Corporate Services communicates to the support departments on the system status through mail, WhatsApp management group and notices and authorizes manual processing.
Action Responsibility	Director Corporate Services, Deputy Director ICT & Innovation

RISK MAPPING

Each risk was mapped based on probability of occurrence and potential impact. Probability and impact were defined as follows.

Probability (Likelihood)

Ran k	Likeliho d/Proba bility	Definition	Colo r code
------------------	--	-------------------	----------------------------

5	Frequent	Likely to occur many times (occurred frequently) Will be continuously experienced unless action is taken to change events.	
4	Likely	Likely to occur sometimes (occurred infrequently) The activity or event expected to occur 50-99% of the time. Will occur often if events follow normal patterns of process or procedure. The event is repeatable and less sporadic.	
3	Occasional	Unlikely, but possible to occur (occurred rarely) An activity or event occurs infrequently, or irregularly, or 25-50% of the time Potential for infrequent occurrence. Events are sporadic in nature Process has higher degree of latent system errors discovered with adequate controls	
2	Seldom	Very unlikely to occur (not known to have occurred) An activity or event that occurs intermittently, or 1-25% of time Not likely to happen (but could) identification during any general or focused review	
1	Improbable	A remote likelihood, being almost inconceivable that event will occur	

Impact

Rank	Impact	Definition	Color code
5	Catastrophic	Massive Equipment destruction. Complete shutdown of systems and related sub-systems System recoverability is impossible within a reasonable period	

		Potential of suspending operations Potential for uncontrollable public relations event	
4	Critical	Destruction of equipment and systems requiring Undefined amount of time to recover. Very large public relations impact requiring large resources to manage information System Deficiencies leading to poor and chronic disruption of operations Potential loss (breakdown) of entire sub-system or sectional operations Shutdown of major operations for a reasonable amount of time.	
3	Moderate	Potential to cause sustained irregular operations until issue is resolved system errors that may pose indirect consequences to the operation Complete shutdown of smaller operations or sections System Deficiencies leading to poor or sporadic disruption to operations. Partial breakdown of an automated system Additional public relations efforts and resources required	
2	Minor	Minor errors in completed Company policy & procedures System errors affecting product quality and / or opportunities for improvement. No equipment damage to slight damage – outcome deferrable with no operational impact. No public relations impact	
1	Negligible	No regulatory violation Breach of Company policy & procedures	

		No public relations impact No equipment damage - no operational impact. System errors present limited opportunities for improvement	
--	--	---	--

Risk Categorization

Each risk was listed and its severity determined based on its probability and impact. From the table below, the risks were categorized into four broad bands of severity as red (extreme), orange (High), Yellow (medium) and blue/green (low).

		Risk Impact (A – F)				
Risk Probability (1 – 5)		Catastrophic A	Critical B	Moderate C	Minor D	Negligible E
	Frequent 5	5*A	5*B	*5C	5*D	5*E
	Likely 4	4*A	4*B	4*C	4*D	4*E
	Occasional 3	3*A	3*B	3*C	3*D	3*E
	Seldom 2	2*A	2*B	2*C	2*D	2*E
	Improbable 1	1*A	1*B	1*C	1*D	1*E

Risk Severity Level Ratings

Based on the risk impact and likelihood as defined above, each of the risks identified were rated as per the table below. The purpose of the rating was to help prioritize the mitigation strategies and the disaster preparedness.

S/ N	System	Risk	Probabili ty	Impac t	Severi ty	Ratin g
1.	IEICS	Staff and client inability to access the IEICS system	Seldom	Critical		Mediu m
2.	SCPVP	Staff and client inability to access the SCPVP system	Seldom	Moder ate		Mediu m
3.	ERP	Staff and client inability to access the ERP system	Seldom	Minor		Low
4.	Email	Staff and client inability to access the Email system	Seldom	Minor		Low

APPENDIX A

ICT Department Call Tree

Serial Number	Caller Title	Call Recipient	Contact Number (Home/Cell Phone/Both)
1	Chief Executive Officer	Mr. H. H. H.	0722222222
2	Chief Executive Officer	Mr. H. H. H.	0722222222
3	Chief Executive Officer	Mr. H. H. H.	0722222222
4	Chief Executive Officer	Mr. H. H. H.	0722222222
5	Chief Executive Officer	Mr. H. H. H.	0722222222
6	Chief Executive Officer	Mr. H. H. H.	0722222222
7	Chief Executive Officer	Mr. H. H. H.	0722222222
8	Chief Executive Officer	Mr. H. H. H.	0722222222
9	Chief Executive Officer	Mr. H. H. H.	0722222222