ARUSHA TECHNICAL COLLEGE



Names: Abbakary M Ukwaju.

Admission no: 18051012026.

Course: Information Technology.

****

**P.O.BOX 9184 DAR ES LAAM**

**PHONE: +2552117816**

**FAX: +255222130390**

**EMAIL: dg@ports.go.tz**

Table of Contents

[**1** **PREFACE** 4](#_Toc74234004)

[**2** **ACKNOWLEDGEMENTS** 5](#_Toc74234005)

[**3** **LIST OF ABBREVIATIONS AND ACRONYMS** 6](#_Toc74234006)

[**4** **INTRODUCTION** 7](#_Toc74234007)

[**5** **Purpose** 7](#_Toc74234008)

[**6** **SCOPE** 7](#_Toc74234009)

[**7** **SERVICES THAT ARE OFFERED BY TANZANIA PORTS AUTHORITIES** 8](#_Toc74234010)

[7.1 CARGO SERVICES 8](#_Toc74234011)

[7.1.1 Dry bulk cargo 8](#_Toc74234012)

[7.1.2 Break bull cargo 8](#_Toc74234013)

[7.1.3 Bulk liquid 8](#_Toc74234014)

[7.2 port stockholders 8](#_Toc74234015)

[**8** **THREAT THAT ARE POSED AGAINST THE TPA** 9](#_Toc74234016)

[8.1 Phishing 9](#_Toc74234017)

[8.2 Sql injection 9](#_Toc74234018)

[8.3 DISTRIBUTED Denial of Service Attack (DDOS) 9](#_Toc74234019)

[8.4 Malwares 9](#_Toc74234020)

[8.5 Social engineering attacks 9](#_Toc74234021)

[**9** **ICT SECURITY PROCEDURES** 10](#_Toc74234022)

[9.1 EDUCATING EMPLOYEE 10](#_Toc74234023)

[9.2 PERSONAL COMPUTER SECURITY 10](#_Toc74234024)

[9.2.1 Passwords 10](#_Toc74234025)

[9.2.2 Good passwords 10](#_Toc74234026)

[9.2.3 Changing passwords 10](#_Toc74234027)

[9.3 Securing your computer when you are away from your desk. 10](#_Toc74234028)

[9.3.1 Lock your computer 10](#_Toc74234029)

[9.3.2 Log out 11](#_Toc74234030)

[9.4 Security While Off-Campus 11](#_Toc74234031)

[9.5 Purchasing laptops, smartphones, tablets and other mobile devices. 11](#_Toc74234032)

[9.6 Mobile device security 11](#_Toc74234033)

[10 Conclusion 11](#_Toc74234034)

# **PREFACE**

This basis for this research originally stemmed from my passion for developing better it security .which will fulfill the mission, vision and value of TPA In truth, I could not have achieved my current level of success without a strong support group. First of all, my parents, who supported me with love and understanding and secondly, my committee members, each of whom has provided patient advice and guidance throughout the research process. Thank you all for your unwavering support.

# **ACKNOWLEDGEMENTS**

During this special time let me use to thank all of the people who played a great role in developing of TPA security police and much thanks should be given to Allah who has given the breath and also other thanks should be given to mr.karyz who have been on my side all the time during different situation and different conditions while writing this police also other thanks to the TPA organization for their corporation in the correction of the information and needed data to be used for writing of the TPA police

# **LIST OF ABBREVIATIONS AND ACRONYMS**

TPA:- Tanzania Ports Authority

TRA :- Tanzania Revenue Authority

DRC:- Democratic Republic of Congo

WMA:- weight measurement agency

TFFA:- Texas food and fuel association

SUMATRA:- Surface and Marine Transport Regulatory Authority

DDOS:- DISTRIBUTED Denial of Service Attack

IT: information technology

# **INTRODUCTION**

The Tanzania Ports Authority (TPA) was established by the Ports Act No. 17 of 2004 as landlord port authority. It operates a system of ports serving the Tanzania hinterland and the landlocked countries of Malawi, Zambia, Democratic Republic of Congo (DRC), Burundi, Rwanda and Uganda.

TPA currently performs the role of both a Landlord and Operator with the main functions of promoting the use, development and management of ports and their hinterlands, entering into contracts for the purpose of delegating the powers of the Authority (through licensing and concessioning ports services).

TPA administers a diverse system of Tanzania’s Mainland sea and inland water ways (Lake Ports). The major sea ports are Dar es Salaam, Tanga and Mtwara while smaller sea ports are Kilwa, Lindi, Mafia, Pangani and Bagamoyo. The lake ports under TPA mandate are: on Lake Victoria include Mwanza North and South Ports, Nansio, Kemondo Bay, Bukoba and Musoma: on Lake Tanganyika, are Kigoma and Kasanga: and on Lake Nyasa are Itungi Port, Kiwira, Manda Liuli and Mbamba Bay.

And the major aim of the tpa are To establish and coordinate system of Harbors, To construct, operate and maintain beacons and other navigational aids, To provide facilities relating to Harbors and provide harbor services and others

# **Purpose**

the main purpose of writing this it security policy if to explain and elaborate which assets at tpa needs to be secured and in which extent dos it requires the security how will it be implemented such us

1. Developing and putting to actions of the rules upon the it infrastructure within the organization

# **SCOPE**

This Policy applies in respect of all I.T-related systems, hardware, services, facilities and processes owned or otherwise made available by the Tanzania Port Authority(TPA) or on its behalf, or which are connected to the TPA network and servers, including for the avoidance of doubt any personally-owned devices that are used in connection with TPA activities (together, I.T. Systems).

# **SERVICES THAT ARE OFFERED BY TANZANIA PORTS AUTHORITIES**

TPA offers different services as follows

## CARGO SERVICES

tpa are well equipped and trained to handle different kind of cargos. Our teams of highly trained professionals in various fields work around the clock to ensure that cargo entering and exiting our ports is in pristine condition and on time.

Cargos are divided into main three parts in atp which are

### Dry bulk cargo

 Dry bulk cargoes cover a range of produce and raw materials that have two features in common: they are unpacked and are homogeneous. These two properties make it easier for dry bulk cargoes to be dropped or poured into the hold of a bulk carrier. Dry bulk cargo such as Rice, wheat, maize, beans, fertilizer, sugar, cement, sodium nitrate, clinkers, gypsum, copper slugs, coal, iron ore and zinc ores.

### Break bull cargo

These are goods that must be loaded individually, including containers. Examples of break bulk cargo that are frequently handled at TPA are iron, steel, metals, motor vehicles & parts, trailers & parts, agri-products, , machinery, copper, railway vehicles, tractor & tractor parts, containers.

### Bulk liquid

Bulk Liquid such as petroleum products, kerosene, diesel, jet oil, and edible oil

## port stockholders

From government agencies to shipping-lines and banks, we work very closely with a number of stakeholders to make your experience with us a smooth as possible, while complying with all the laws and regulations involved in import and export through our ports. eg TRA,TZR,WMA,TFFA,SUMATRA and others

# **THREAT THAT ARE POSED AGAINST THE TPA**

Most of organizations in the world are not safe from cyber-attacks and threats most of the cybercrimes based on the use of sophisticated technologies in this case no any organization or business that feels more secure from different attacks

Security threat:- is a **malicious**and **intended or not intended attack** by an individual or organization to gain unauthorized access to another individual’s or organization’s network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.

Threats are posedagainst the tpa are

## PHISHING

this is sending of malicious email which seems to come from trusted sources because there are some of people emails that are shown to the email so this can also facilitate the attacker to use phishing

## SQL INJECTION

structured query language injection attack this is the attack where the attacker attempt to access data base by using of malicious sql scrips and when the attacker succeeds he can delete update the database and its don if there are fields where user can put information such as user names and other forms

## DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

 Aim to disrupt a computer network by flooding the network with superfluous requests to overload the system and prevent legitimate requests being fulfilled.

## MALWARES

Even if there is fire wall or same viruses and malware do sometimes get through. In fact, even when security software is installed, users sometimes turn it off or change its settings if they feel like it’s interfering there activities.

## SOCIAL ENGINEERING ATTACKS

This is the attack where the attacker acts like your friend but he or she need just a piece of information from your or he need to use you to get in your organization for TPA there are sane employees who have used their name and email in different social media accounts this can be used as one way that hackers can use the employee to gat in in the organization

# **ICT SECURITY PROCEDURES AGAINST**

Most of it security threats are caused by different attackers but also there are same causes of those attacks such use the users of the system and also the programmers of the system did the activity of developing the system and did not put into consideration about the security of the system.

Regarding to the above threats that I have explained there are things to be considered by the management and the it professions

## EDUCATING EMPLOYEE

The employee in the organization should be educated about security and the sensitiveness of the information that belong to the organization and how to prevent themselves from different attacks

## PERSONAL COMPUTER SECURITY

### Passwords

Passwords are the key to many systems and applications. A password helps to prove identity, and to ensure personal privacy and helps to protect the privacy of the data being accessed. Poor passwords compromise security. Passwords must comply with the advice in the following sections.

### Good passwords

A good password is one that is difficult to guess. Current best practice is to use a ‘passphrase’ made up of three random words, rather than a single word password. A good password is one that can be remembered easily and typed in quickly so that anyone looking on the other side will not be able to see what you are typing. A password must at list fulfill the following;

* be at least sixteen characters long
* contain at least one upper case and one lower-case letter
* not appear in any dictionary or any other list
* have no personal connection with the owner

### Changing passwords

If you have a strong passphrase as stated above, you do not need to regularly change your password. However, if you think your account has been compromised then you should change your password immediately

## Securing your computer when you are away from your desk.

When a computer is left unattended, it is essential that that no unauthorized person can gain access to it. There are a number of simple techniques that should be used to prevent from the unauthorized access

### Lock your computer

by pressing windows and L

### Log out

This will prevent any access until a valid username and password is entered.

## Security While Off-Campus

## Purchasing laptops, smartphones, tablets and other mobile devices.

There are several additional checks that must be performed when a mobile device is purchased. It is the responsibility of the person arranging the purchase to find out if the customer intends to use the portable device to hold or access sensitive or confidential data. If so, encryption must be used (see below). Any data must be stored in such a way that it can easily be backed up or identified for encryption. Any data of value to the tpa must be placed on secure institutional storage. IT Support or local technical staff will be able to advice on the best way to achieve this.

## Mobile device security

Employees of university owned mobile devices should follow those things

* Mobile devices must be treated as carefully as if they were the employee’s own property
* Mobile device security is the responsibility of the employee
* Mobile devices must be securely locked away when not in use and must not be left unattended in a public place.
* Mobile devices must not be left within sight of ground floor windows or within easy access of external doors.

# **Conclusion**

This police if is followed as explained it will save the above attacks and also will reduce the cost to the organization.