

KCA UNIVERSITY

BAC 1305 Research Skills and Design

**NAMES**

1. Duncan Mburu – 20/04711
2. Francis Ngugi – 20/04744
3. Julius Ngau – 20/
4. Ste
5. Adonijah kiolimo - 20/02931

SUPERVISOR: Mr. Peter Kiarie

**TITLE**

**COMPUTER LAB SECURITY MANAGEMENT SYSTEM**

**Declaration**

We hereby declare that this is our own work and has not been previously included in a thesis or dissertation submitted to this or any other institution. We have followed the guidelines provided by the university in writing the report. Whenever we have used materials (data, theoretical analysis, and text) from other sources, we have given due credit to them in the text of the report and giving their details in the references.

**Table of Contents**

[**1 Background** 2](#_Toc87525204)

[**2 Problem statement** 3](#_Toc87525205)

[**3 Proposed solution** 4](#_Toc87525206)

[**4.1 General Objective** 5](#_Toc87525207)

[**4.2 Specific Objectives** 5](#_Toc87525208)

# **1 Background**

The need to use computers in organizations has grown over the decades for their significant effect in the organizations. With the increased demand of computers in organizations, computer related crimes becomes a common issue. This has led to the need of a Computer Lab Security System that will limit theft cases and ensure that the computers and related resources are safe by protecting them from physical and natural calamities.

# **2 Problem statement**

The implementation of the Computer Lab Security Management System will make the running and maintenance of the computer labs easier for any problem that would cause a disruption in the lab will be handled efficiently thus minimal financial risk in the long run to the organization.

The following problems arise especially when dealing with large number of people:

1. **Theft** - Recently, there have been many stolen or lost computers, USB memory sticks, and other items at Nagoya University. Computer theft can lead to information leaks of stored data as well as article damage. In particular, if important data, such as personal information, etc., is stored in the computer, the damage can be serious.

Therefore, preventive measures against information leaks due to theft are just as important as physical anti-theft measures. Even if a logon password is set for the OS, if the hard disk is physically removed and connected to another computer, the data can easily be viewed. Consequently, it is necessary to take other preventive measures, such as data encryption, etc., in addition to setting a password.

1. **Fire** - A fire in a data center or computer room could be devastating for your organization. Not only is there the risk of personal injury or loss of life, but you could also lose all your data and equipment—and with it, your entire organization. Even the downtime and loss of productivity caused by a fire could cost you thousands.
2. **Computer viruses** - Computer viruses are programs that replicate themselves to spread to other computers; they have the potential of altering the behavior of their computer hosts. They can destroy research and instructional data and computer equipment, and they can easily be spread by honest, unknowing individuals, who are themselves using the host computers appropriately.

A computer virus can affect any laboratory in which honest individuals are using programs imported from other sources. Viruses can be spread through the normal use or installation of commercial software, as well as through malicious intent. It is important to remember that in most cases, viruses have been spread unintentionally by people who did not mean to harm the computer systems they operate.

# **3 Proposed solution**

After careful analysis of the problem at hand, the solution that will be best solve the problems is through the implementation of Computer Lab Security Management System that will automate the managerial activities in the following ways:

1. Install Anti-theft alarms that goes off any time an input device is ejected from the computer.
2. Installing Fire alarms that signals admins in case of a fire outbreak.
3. Installing antivirus that detects any corrupted input device inserted in the computers and blocks any further operation to avoid data loss.

**4** **Objectives**

## **4.1 General Objective**

Coming up with a system that will automate the activities in computer lab management and make it easier for users to remain updated in real time in case of danger.

## **4.2 Specific Objectives**